USB Deviceserver & USB Dongleserver

myUTN ユーザーマニュアル Linux

USB Deviceserver：
myUTN-50a、myUTN-55、myUTN-2500

USB Dongleserver：
myUTN-80、myUTN-800

メーカと窓口

SEH Computertechnik GmbH
Suedring 11
33647 Bielefeld
Germany (ドイツ)
電話：+49 (0)521 94226-29
FAX：+49 (0)521 94226-99
サポート：+49 (0)521 94226-44
電子メール：info@seh.de
ホームページ：http://www.seh-technology.jp

文書

種類：ユーザーマニュアル
myUTN ユーザーマニュアル Linux
バージョン：4.1 | 2021-07

法律情報

目次

1 一般情報

1.1 製品

目的

UTN サーバは、USB Deviceserver と USB Dongleserver から構成されます。TCP/IP ネットワークを介し、USB Deviceserver の場合はネットワーク非対応の USB デバイス (USB ハードディスクドライブ、USB プリンタ、など) が利用でき、USB Dongleserver の場合はネットワーク非対応の USB ドングルが利用できます。使用する USB デバイスや USB ドングルを UTN サーバの USB ポートに接続すると、UTN (UTN = USB to Network) 機能に対応するソフトウェアツールの「SEH UTN Manager」により、USB デバイスや USB ドングルとクライアント間に仮想の USB 接続が確立されます。接続された USB デバイスや USB ドングルは、ローカル接続とまったく同じ状態で使用できます。

重要：

Dongleserver myUTN-80 と myUTN-800 は、USB ドングル専用に設計されました。

重要：

USB ドングルおよび USB デバイスは、以降「USB デバイス」と呼びます。

システム要件

UTN サーバは、TCP/IP ネットワークで使用するよう設計されています。

SEH UTN Manager は、次のシステムで実行できます。

- Microsoft Windows (32/64-Bit; Windows 10 以降以降以降以降 以降 , Server 2012 R2 以降)
- macOS 10.9 以降以降 以降以降 [1]
- Linux (Debian 10, Ubuntu 20.0.4, Red Hat Enterprise Linux 8, Oracle 8, CentOS 8, SUSE Linux Enterprise 15.1, openSUSE Leap 15.1) [2]
- IPv4 TCP/IP ネットワーク

1. macOS 11.x (Big Sur)では、USBデバイスのサポートが制限されており、Apple Silicon (Apple M1チップ)ベースのMacでは動作しません。
2. Linuxシステムは多種多様であるため、インストールの成功は保証できません。インストールはお客様ご自身の責任で行ってください。

重要：
アイソクロナス USB デバイス (カメラ、マイク、スピーカなど) への対応は次の環境に依存します。

- オペレーティングシステム：
  - Windows
  - Linux
- UTN サーバモデル
  (各製品情報を参照してください。)
- ソフトウェアバージョン
  - UTN サーバのファームウェア / ソフトウェア：14.5.5 以降
  - SEH UTN Manager：3.1.4 以降

このマニュアルは Linux 環境での使用について説明します。他の環境での使用については、該当するシステム用のユーザーマニュアルを参照してください。詳細は、「説明書」⇨ 🗎3 の章を参照してください。

関連製品との組合せ

UTN サーバを他の SEH Computertechnik GmbH 製品と組み合わせることで、デバイスを環境に合わせて理想的に使用することができます。

Service^{plus}

myUTN-80 および myUTN-800 Dongleserver のサービス契約には、Service^{plus} パッケージが利用できます。Service^{plus} パッケージでは、Dongleserver のメーカ保証を 36 ヶ月から 60 ヶ月に延長します。また、製品に不具合がある場合は、先出しの代替品をすぐに受け取ることができます。Service^{plus} パッケージは別途購入が必要です。
詳細情報：

http://www.seh-technology.jp/services/service-packages.html

ラックマウントキット

Dongleserver を完全かつ安全に保管するためには、Rack Mount Kit (RMK) を推奨します。このインストールキットにより、Dongleserver を 19 インチのサーバラックに取り付けることができます。
詳細情報：

http://www.seh-technology.jp/products/rack-mount-kits.html

1.2 説明書

最新の説明書は、当社の次のウェブサイトからダウンロードしてください：http://www.seh-technology.jp

該当する説明書

UTN の説明書は、次のように構成されています。

クイック・インストール案内	印刷、PDF	安全に関する情報、技術データ、ハードウェア設置に関する説明、適合宣言
ユーザーマニュアル	PDF	UTN の設定および管理についての詳細な説明。次のシステムに関して、システム固有の説明をしています。 ・Windows ・macOS ・Linux
オンラインヘルプ	HTML	ウェブインターフェイス「myUTN Control Center」の使用方法についての情報。 **(オンラインヘルプは、ウェブインターフェイスのメニューの一部でダウンロードは必要ありません。)**
製品情報	印刷、PDF	機能および技術データ
パンフレット	印刷、PDF	
Open Source 使用許諾	オンライン	http://www.seh-technology.jp/services/licenses.html

記号および凡例

本書では、様々な記号と表記が使用されています。

警告
警告

警告には、細心の注意が必要な重要な情報が含まれます。警告に従わない場合、誤動作することがあります。

重要：
重要な情報

このメモには、正常動作に関する重要な情報が含まれます。

✓ 必要事項	操作を始める前に準備が必要な要件を示します。
• 箇条書き（ブレット）	リスト
1. 箇条書き（番号）	手順の説明
↳ 結果	実行した操作の結果
ヒント	推奨事項および役立つアドバイス
⇨🗎	参照 (説明書内でハイパーリンクが使用できます。)
太字	ボタン名、メニュー項目、選択項目などの画面の用語
`Courier`	(コマンドライン、スクリプトなどのコード、パス名。
「固有名」	固有名は、「」内に示します。

1.3 サポートとサービス

SEH Computertechnik GmbH では広範囲なサポートを提供しています。ご質問がある場合は、当社の窓口までご連絡ください。

月曜 ～ 木曜	午前 8:00 ～ 午後 4:45
金曜	午前 8:00 ～ 午後 3:15

+49 (0)521 94226-44

support@seh-technology.jp

製品に関する情報は、すべて当社の次のウェブサイトからダウンロードできます：

http://www.seh-technology.jp

1.4 安全の確保

本書やパッケージ、デバイス本体に記載された安全規定および警告は、すべて読み遵守してください。誤った使用方法を避けることで、人体への悪影響や製品の故障を防ぐことができます。

目的用途

UTN サーバは、TCP/IP ネットワーク上で使用します。また、オフィス環境での使用を意図して設計されています。ネットワークユーザは、このサーバによりネットワーク非対応の USB デバイスを利用することができます。

不正使用

myUTN の説明書に記載されている機能に適合しないデバイスの使用は、すべて不正使用とみなされます。

安全規定

UTN サーバを初めてセットアップする前に、「クイック・インストール案内」の安全規定を読み遵守してください。この説明書は、印刷物としてパッケージに同梱されています。

警告

本書に記載されたすべての警告を読み遵守してください。警告は、危険と判断される操作説明の箇所に、次のように表記されています。

警告

警告！

責務および保証

安全規定と警告を遵守しなかった結果による、人への傷害や財産の損失および間接的損害について、SEH Computertechnik GmbH は一切の責任を負いません。遵守しなかった場合はまた、保証に関する申し立ては無効となります。

デバイスの改造と修理

ハードウェアおよびソフトウェアの改造やデバイスの修理は許可されていません。デバイスの修理が必要な場合は、当社サポートまでご連絡ください。⇨ 🗎4

1.5 最初のステップ

1. 人への傷害およびデバイスへの損傷を避けるため、セキュリティ規定を読み遵守ください。⇨ 🗎4
2. ハードウェアを設置します。ハードウェアの設置には、UTN サーバのネットワークと USB デバイス、電源への接続が含まれます。⇨ 🕮 「クイック・インストール案内」
3. ソフトウェアをインストールします。ソフトウェアのインストールには、必要な「SEH UTN Manager」ソフトウェアツールをクライアントにインストールし、IP アドレスを割り当てる作業が含まれます。⇨ 🕮 「クイック・インストール案内」
4. 最適な形でネットワークに組み込み、十分に保護されるように UTN サーバを設定してください。設定方法はすべて、この説明書に説明されています。
5. SEH UTN Manager は、UTN サーバに接続された USB デバイスへの接続を確立し管理するために使用します。⇨ 🗎33

UTN の説明書に関する情報は、「説明書」⇨ 🗎3 の章を参照してください。

2 管理方法

UTN サーバは、いくつかの方法で管理、設定および保守することができます。

- myUTN Control Center による管理 ⇨ 🗎6
- SEH UTN Manager による管理 ⇨ 🗎8 電子メールによる管理 ⇨ 🗎14

2.1 myUTN Control Center による管理

UTN サーバには、ユーザインターフェイスである myUTN Control Center が装備され、インターネットブラウザ (Mozilla Firefox など) で起動できます。

UTN サーバは、myUTN Control Center から設定、監視および保守することができます。

- myUTN Control Center をブラウザで起動する ⇨ 🗎6
- myUTNSEH UTN Manager から Control Center を起動する ⇨ 🗎6
- 制御機器 ⇨ 🗎7

myUTN Control Center をブラウザで起動する

✓ UTN サーバがネットワークと電源に接続されていること。
✓ UTN サーバに有効な IP アドレスが設定されていること。⇨ 🗎16

1. ブラウザを開きます。
2. UTN サーバの IP アドレスを URL に入力します。

↳ myUTN Control Center がブラウザに表示されます。

重要：
myUTN Control Center が表示されない場合は、ゲートウェイが設定されていることを確認し (⇨ 🗎16)、ブラウザのプロキシ設定も確認してください。

myUTNSEH UTN Manager から Control Center を起動する

✓ UTN サーバがネットワークと電源に接続されていること。
✓ UTN サーバに有効な IP アドレスが設定されていること。⇨ 🗎16
✓ SEH UTN Manager がクライアントにインストールされていること。⇨ 🗎8

1. SEH UTN Manager を起動します。
2. 選択リストから UTN サーバを選択します。
3. メニューバーから、**UTN サーバ – 構成**を選択します。

↳ ブラウザが起動して、myUTN Control Center が表示されます。

制御機器

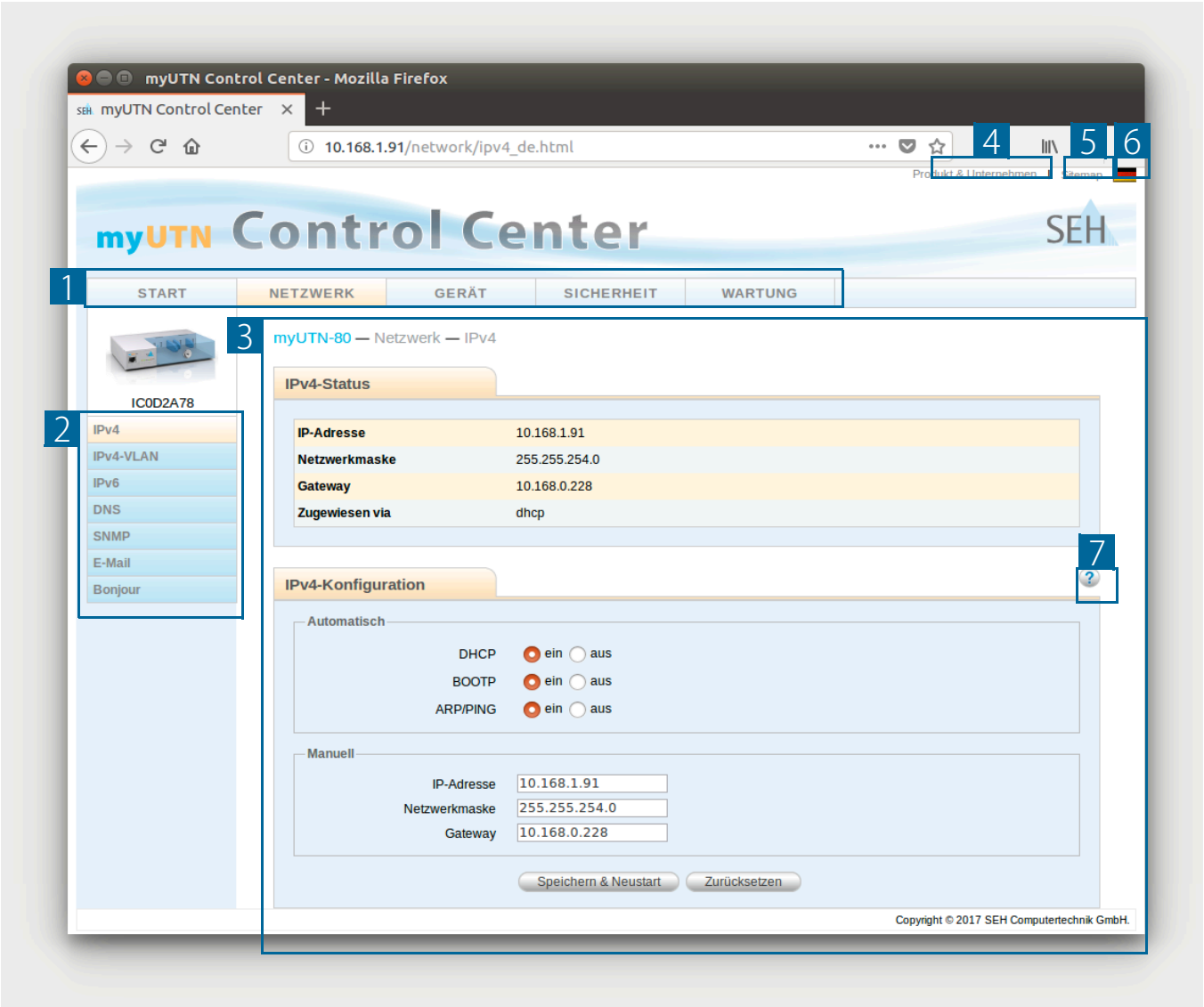


図 1： myUTN Control Center

1	メニュー項目	メニュー項目を選択 (マウスをクリック) すると、使用可能なサブメニューが左側に表示されます。
2	サブメニュー項目	サブメニューの項目を選択すると、対応するページとその内容が表示されます。
3	ページ	メニューの内容
4	製品と会社情報	メーカの連絡先および製品の詳細情報
5	サイトマップ	myUTN Control Center の全体図が表示され、myUTN Control Center のすべてのページに直接アクセスできます。
6	フラグ	言語の選択
7	？アイコン	オンラインヘルプ

2.2 SEH UTN Manager による管理

「SEH UTN Manager」は、SEH Computertechnik GmbH が開発したソフトウェアツールです。SEH UTN Manager は、UTN サーバに接続された USB デバイスへの接続を確立し管理するために使用されます。

機能

このソフトウェアは、ネットワーク内の USB デバイスを使用するクライアントすべてにインストールします。SEH UTN Manager を起動すると、ネットワークをスキャンして、接続された UTN サーバを検出します。検出されたすべての UTN サーバとそのサーバに接続された USB デバイスが選択リストに表示されます。UTN サーバに接続された USB デバイスを使用するには、UTN サーバを「選択リスト」に追加します。選択リストに表示されたデバイスを管理して、接続された USB デバイスを使用することができます。SEH UTN Manager の操作については、「SEH UTN Manager の操作」⇨ 🗎33 の章で詳しく説明します。

警告

UTN (⇨ 🗎1) と対応する SEH UTN Manager は IPv4 ネットワークでのみ機能します。

IPv6 単独のネットワークでは myUTN Control Center (⇨ 🗎6) のみが UTN サーバの管理に利用できます。

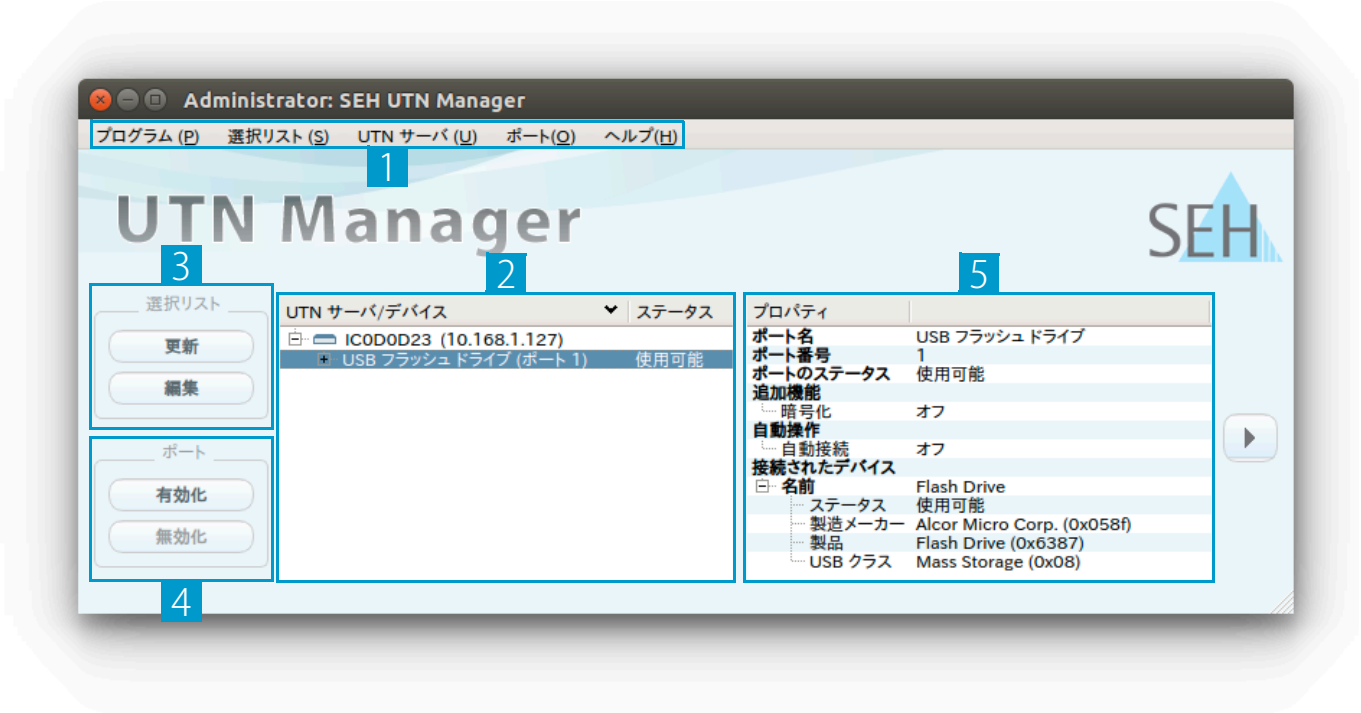


図 2： SEH UTN Manager

1	メニューバー	利用できるメニュー項目
2	選択リスト	選択された UTN サーバと接続された USB デバイスを表示します。
3	選択リスト編集用ボタン	ネットワーク上で UTN サーバを検索し、任意のデバイスを選択するためのダイアログを起動します。⇨ 🗎33
4	ポート接続管理用ボタン	USB ポート (⇨ 🗎35) に接続された USB デバイスへの接続を確立、または接続 (⇨ 🗎36) を中断します。
5	プロパティ表示領域	選択された UTN サーバ、または USB デバイスの情報を表示します。⇨ 🗎38

SEH UTN Manager の使用方法の詳細は、⇨ 🕮「SEH UTN Manager オンラインヘルプ」を参照してください。オンラインヘルプを起動するには、SEH UTN Manager のメニューバーから、**ヘルプ – オンラインヘルプ** を選択します。

重要：

SEH UTN Manager の一部の機能は表示されない、または非アクティブとして表示される場合があります。それは、次の要因に依存します。

- 選択リストの種類と場所
- クライアント側のユーザ権限およびグループのメンバシップ
- クライアントのオペレーティングシステム
- 製品に固有なセキュリティメカニズムの設定
- UTN サーバおよび各 USB ポートの状態

詳細は、「SEH UTN Manager – 機能の概要」⇨ 🗎93 の章を参照してください。

バージョン

SEH UTN Manager には 2 つのバージョンがあります。

- フルバージョン：
  グラフィカルユーザインターフェイス (⇨ 図 2 🗎8) と詳細な機能を備えた SEH UTN Manager です。
- ミニマルバージョン (グラフィカルユーザインターフェイスなし)
  コマンドライン (「utnm」⇨ 🗎42) ⇨ 🗎37 のみを使用します。

重要：

一般にはフルバージョンの使用を推奨します。

ミニマルバージョンは上級者のみが使用してください。

両方のバージョンとも、「SEH UTN Service」(デーモン) がバックグラウンドで動作しシステム起動後に自動的にアクティブになります。

さらに、次のユーザグループが区別されます。

- 管理者権限のあるユーザ (管理者)
- 管理者権限のないユーザ (標準ユーザ)

重要：

機能によっては管理者だけが設定できます。詳細は、「SEH UTN Manager – 機能の概要」⇨ 🗎93 の章を参照してください。

インストール

SEH UTN Manager を使用するには、プログラムを Linux オペレーティングシステムのコンピュータにインストールする必要があります。SEH UTN Manager のインストールファイルは、SEH Computertechnik GmbH の次のウェブサイトにあります：

http://www.seh-technology.jp/services/downloads.html

以上以上以上以上以上 Linux システム (64 ビット) では次のインストールパッケージが利用できます。

- *.deb (64 ビット Debian ベースシステム用)
- *.rpm (64 ビット Red Hat ベースシステム用)

警告

Linux システムには数多くの種類があるため、すべての Linux システムでの正常なインストールは保証されていません。

各自の責任でインスールを実行してください。

SEH Computertechnik GmbH は、ご要求に応じて有償でインストールをサポートしています。⇨ 4

次の 64 ビットシステムで正常なインストールを検証しています。

- Debian: Debian10, Ubuntu 20.0.4
- Red Hat: Red Hat Enterprise Linux 8, Oracle 8, CentOS 8, openSUSE Leap 15.1

インストール要件：

✓ deb: Linux kernel 2.6.32 or later, glibc 2.15 or later, DKMS (ダイナミックカーネルモジュール対応)

✓ rpm: Linux kernel 2.6.32 or later, glibc 2.12 or later, DKMS (ダイナミックカーネルモジュール対応)

インスールパッケージは 4 つあります。

1) ドライバ
2) サービス (SEH UTN service/ デーモン)
3) clitool (コマンドラインインターフェイスツール「utnm」)
4) manager (グラフィカルユーザインターフェイス)

インストールされたパッケージの数で、SEH UTN Manager のバージョンが判定されます。

パッケージ 1) ～ 3)：ミニマルバージョン

パッケージ 1) ～ 4)：フルバージョン

重要：

バージョンに従い、上記の順序でパッケージをインストールしてください。

ファイルのインストールはディストリビューションに依存します。詳細は、オペレーティングシステムの説明書を参照してください。

重要：

インストールは、経験のあるユーザのみが実行してください。

以下にインストール例をいくつか示します。

- 「SEH UTN Manager を Ubuntu 20.0.4.x LTS (64 ビット) に Software Management からインストールする」⇨ 🗎11
- 「SEH UTN Manager を Ubuntu 20.0.4.x LTS (64 ビット) に端末からインストールする」⇨ 🗎11
- 「SEH UTN Manager を Red Hat Enterprise Linux Server (7.4) にインストールする」⇨ 🗎12

重要：

Linux 関連の詳細なインストール情報を含む知識ベースの記事 (例えば、DKMS のインストールと UEFI セキュアブートの問題) に SEH Computertechnik GmbH のウェブサイトからアクセスできます

http://www.seh-technology.com/services/knowledgebase.html

SEH UTN Manager を Ubuntu 20.0.4.x LTS (64 ビット) に Software Management からインストールする

✓ Linux カーネル 2.6.32 以降
✓ glibc 2.15 以降
✓ OpenSSL 1.0.1 以降
✓ DKMS (Dynamic Kernel Module Support) がクライアントにインストールされていること。
✓ 使用ユーザが、`sudo` コマンドによりルート特権を獲得できること。

1. 1 番目のインストールパッケージを起動します。
   Ubuntu ソフトウェアが表示されます。
2. **インストール**をクリックします。
   パスワードのプロンプトが表示されます。
3. パスワードを入力してください。
   パッケージがクライアントにインストールされます。
4. 残りのパッケージについて、ステップ 1 から 3 を繰り返し実行します。
5. インストールに使用したアカウントのユーザは、自動的にクライアント上で SEH UTN Manager を使用できます。他のユーザが SEH UTN Manager を使用できるようにするには、そのユーザを「utnusers」グループに追加します。そのために、**端末**を起動して次のコマンドを入力します：
   `sudo usermod -aG utnusers <ユーザ名>`
6. 一度ログアウトして再度ログインすると、グループの変更が有効になります。

↳ SEH UTN Manager がクライアントにインストールされます。SEH UTN Manager (⇨ 🗎13) を起動し、接続した USB デバイスを含む USB ポートへの接続をアクティブにすることで、インストールされたことを確認します。詳細は「SEH UTN Manager の操作」⇨ 🗎33 の章を参照してください。

SEH UTN Manager を Ubuntu 20.0.4.x LTS (64 ビット) に端末からインストールする

✓ Linux カーネル 2.6.32 以降
✓ glibc 2.15 以降
✓ OpenSSL 1.0.1 以降
✓ DKMS (Dynamic Kernel Module Support) がクライアントにインストールされていること。
✓ 使用ユーザが、`sudo` コマンドによりルート特権を獲得できること。

1. **端末**を開きます。
2. カーネル用のヘッダをインストールします：

```
sudo apt-get install linux-headers-`uname -r`
```

3. カーネルとヘッダのバージョン番号が完全に一致していること確認します。
   カーネル：`uname -r`
   ヘッダ：`sudo apt list --installed | grep linux-headers`

警告

バージョン番号は同一である必要があります。異なる場合は、SEH UTN Manager パッケージを正しくインストールできません。

カーネルとヘッダが一致していない場合は、独自で一致するように編集して作成する必要があります。

4. SEH UTN Manager のパッケージがあるディレクトリに移動します：
   `cd <ディレクトリ>`
5. 必要な　SEH UTN Manager パッケージをインストールします：
   `sudo dpkg -i <フルパッケージ名>`
6. インストールに使用したアカウントのユーザは、自動的にクライアント上で SEH UTN Manager を使用できます。他のユーザが SEH UTN Manager を使用できるようにするには、そのユーザを「utnusers」グループに追加します：
   `sudo usermod -aG utnusers <ユーザ名>`
7. 一度ログアウトして再度ログインすると、グループの変更が有効になります。

↳ SEH UTN Manager がクライアントにインストールされます。SEH UTN Manager (⇨ 🗎13) を起動し、接続した USB デバイスを含む USB ポートへの接続をアクティブにすることで、インストールされたことを確認します。詳細は「SEH UTN Manager の操作」⇨ 🗎33 の章を参照してください。

SEH UTN Manager を Red Hat Enterprise Linux Server (7.4) にインストールする

✓ Linux カーネル 2.6.32 以降
✓ glibc 2.12 以降
✓ OpenSSL 1.0.1 以降
✓ DKMS (Dynamic Kernel Module Support) がクライアントにインストールされていること。
✓ 使用ユーザが、`sudo` コマンドによりルート特権を獲得できること。

1. **端末**を開きます。
2. カーネル用のヘッダをインストールします：
   `sudo yum install kernel-devel-`uname -r``
3. カーネルとヘッダのバージョン番号が完全に一致していること確認します。
   カーネル：`uname -r`
   ヘッダ：`sudo yum list | grep kernel-headers`

警告

バージョン番号は同一である必要があります。異なる場合は、SEH UTN Manager パッケージをインストールできません。

カーネルとヘッダが一致していない場合は、独自で一致するように編集して作成する必要があります。

4. SEH UTN Manager のパッケージがあるディレクトリに移動します：
   `cd <ディレクトリ>`
5. 必要な　SEH UTN Manager パッケージをインストールします：
   `sudo yum install <フルパッケージ名>`
6. インストールに使用したアカウントのユーザは、自動的にクライアント上で SEH UTN Manager を使用できます。他のユーザが SEH UTN Manager を使用できるようにするには、そのユーザを

「utnusers」グループに追加します：
`sudo usermod -aG utnusers <ユーザ名>`

7. 一度ログアウトして再度ログインすると、グループの変更が有効になります。

↳ SEH UTN Manager がクライアントにインストールされます。SEH UTN Manager (⇨ 🗎13) を起動し、接続した USB デバイスを含む USB ポートへの接続をアクティブにすることで、インストールされたことを確認します。詳細は「検索パラメータを設定する」⇨ 🗎33 の章を参照してください。

プログラムの起動

SEH UTN Manager を起動するには、ランチャから Dash (検索) により「UTN Manager」を呼び出して、**端末**から `utnmanager` コマンドを実行します。

更新

プログラムの更新を手動または自動で確認できます。詳細は ⇨ 🕮「SEH UTN Manager オンラインヘルプ」で確認してください。

2.3 電子メールによる管理

UTN サーバを電子メールにより管理することで、インターネットを使用 (リモートアクセス) できる任意のコンピュータから管理することができます。

- UTN サーバステータスの取得
- UTN サーバパラメータの取得
- UTN サーバの更新

そのためには、コマンドを電子メールのヘッダに書き込みます。⇨ 表 1 🗎14

表1： コマンドとコメント：

コマンド	オプション	説明
< コマンド >	`get status`	UTN サーバステータスページを取得します。
	`get parameters`	UTN サーバパラメータリストを取得します。
	`set parameters`	UTN サーバに採用される少なくとも 1 つのパラメータを UTN サーバに送信します。 パラメータとその値を電子メールの本文に書き込みます。 < パラメータ > = < 値 > 構文と値はパラメータリストから検出できます。⇨ 🗎69
	`update utn`	メールに添付したソフトウェアにより、自動更新を実行します。
	`help`	リモートメンテナンス情報のページを取得します。
[< コメント >]		説明用の任意のテキスト文。

命令の表記規約は次のとおりです。

- 大文字、小文字を区別しない
- 複数の空白文字を許可
- 最大長：128 バイト
- ASCII フォーマットのみ読み込み可能

また、更新を実行またはパラメータを変更するために TAN を実行する必要があります。開始するには、TAN を含むステータスページ (⇨ 表 1 🗎14) を電子メールで取得する必要があります。受信した TAN を電子メールの本文に入力します。その後に、空白文字を 1 字入れます。

✓ DNS サーバが UTN サーバ⇨ 🗎21 上で設定されていること。
✓ 電子メールが受信できるように、UTN サーバに POP3 サーバ上の電子メールアドレスが設定されていること。
✓ POP3 と SMTP のパラメータが UTN サーバ上で設定されていること。⇨ 🗎23

1. 電子メールのプログラムを起動します。
2. 新しい電子メールを作成します。
   - 受信者として UTN アドレスを入力します。
   - 件名に命令を入力します。`cmd:` < コマンド > `[`< コメント >`]`
     コマンドとコメント：⇨ 表 1 🗎14.
   - TAN の適用が可能な場合は、それを電子メールの本文に入力します。
3. 電子メールを送信します。

↳ UTN サーバがその電子メールを受信し、命令を実行します。

例

UTN サーバパラメータリストを取得する場合

宛先：`UTNserver@company.com`

件名：`cmd: get parameters`

「設定」パラメータリストを設定する場合

宛先：`UTNserver@company.com`

件名：`cmd: set parameters`

メール本文：
```
TAN = nUn47ir79Ajs7QKE
sys_descr = <Your description>
```

3 ネットワーク設定

UTN サーバをネットワークに最適な形で組み込むには、次のように設定してください。

- IPv4 パラメータの設定方法 ⇨ 🗎16
- 設定が保存されます。IPv6 パラメータの設定方法 ⇨ 🗎18
- WLAN を設定する方法 ⇨ 🗎19
- DNS を設定する方法 ⇨ 🗎21
- SNMP の設定方法 ⇨ 🗎21
- Bonjour の設定方法 ⇨ 🗎22
- 電子メール (POP3 と SMTP) を設定する方法 ⇨ 🗎23
- VLAN 環境での UTN サーバの利用方法 (myUTN-80 以降のみ) ⇨ 🗎25

3.1 IPv4 パラメータの設定方法

ハードウェアのインストールで (ð &「ハードウェアインストールガイド」)、UTN サーバはネットワークに接続されます。UTN サーバは、次に IP アドレスが BOOTP (Bootstrap Protocol) または DHCP (Dynamic Host Configuration Protocol) ブートプロトコルにより動的に取得されているかを確認します。いずれの方法でも取得できない場合、INU サーバは Zeroconf により、Zeroconf に予約されたアドレス範囲 (169.254.0.0/16) から自らに IP アドレスを割り当てます。

重要：
UTN サーバは、IPv6 ネットワークに接続している場合、IPv6 アドレスを追加で受信します。⇨ 🗎18

UTN サーバに割り当てられた IPv4 アドレスは、「SEH UTN Manager」ソフトウェアツールにより検出することができます。この手順は通常、初期セットアップ時に実行します (ð &「クイック・インストール案内」)。

UTN サーバを適切な形で TCP/IP ネットワークに組み込むために、様々な IPv4 パラメータの設定や、静的 IP アドレスを手動で UTN サーバに割り当てることもできます。

- IPv4 アドレスを SEH UTN Manager から決定して IPv4 パラメータを設定する ⇨ 🗎17myUTN Control Center から IPv4 パラメータを設定する ⇨ 🗎16
- SEH UTN Manager から IPv4 アドレスを設定する ⇨ 🗎17

IPv4 アドレスを SEH UTN Manager から決定して IPv4 パラメータを設定する ⇨ 🗎**17myUTN Control Center から IPv4 パラメータを設定する**

1. myUTN Control Center を起動します。
2. **ネットワーク** – **IPv4** を選択します。
3. IPv4 パラメータを設定します。⇨ 表 2 🗎17
4. **保存して再起動する**をクリックして確定します。

↳ 設定が保存されます。

表2： IPv4 パラメータ

パラメータ	説明
DHCP BOOTP ARP/PING	DHCP、BOOTP、ARP/PING プロトコルを、有効または無効にします。 DHCP および BOOTP による IP アドレスの割り当ては、これらのプロトコルの 1 つがネットワークに実装されている場合、自動的に実行されます。 Zeroconf によって割り当てられた IP アドレスを変更するには、ARP および PING コマンドを使用することができます。この実装状況は、システムにより異なります。使用するオペレーティングシステムの説明書を参照してください。 UTN サーバへの IP アドレス割り当て後は、これらのオプションを無効にすることを推奨します。
IP アドレス	UTN サーバの IP アドレスです。
サブネットマスク	UTN サーバのサブネットマスクです。 サブネットマスクは、大規模なネットワークの論理的なサブネットワークへの分割に使用します。UTN サーバをサブネットワークで使用する場合は、サブネットワークのサブネットマスクが必要です。
ゲートウェイ	UTN サーバが使用するネットワークの標準ゲートウェイの IP アドレスです。 ゲートウェイにより、外部ネットワークから IP アドレスを指定できます。

SEH UTN Manager から IPv4 アドレスを設定する

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること ⇨ 🗎8。
✓ UTN サーバが選択リストに表示されていること ⇨ 🗎33。

1. SEH UTN Manager を起動します。
2. 選択リストから UTN サーバを選択します。
3. メニューバーから、**UTN サーバ – IP アドレスの設定**を選択します。
   IP アドレスの設定ダイアログが表示されます。
4. 関連する TCP/IP パラメータを入力します。
5. **OK** をクリックします。

↳ 設定が保存されます。

IPv4 アドレスを SEH UTN Manager から決定して IPv4 パラメータを設定する

SEH UTN Manager は、接続された INU サーバをネットワークから検索します。

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること ⇨ 🗎8。

1. SEH UTN Manager を起動します。
2. **選択リストに何も入力されていません。**ダイアログに対して、**はい**で確認します。
   このダイアログが表示されず、メインのダイアログ画面が表示される場合は、メニューバーで選択リスト - 編集を選択します。
   選択リストの編集ダイアログが表示されます。
3. ネットワークリストから INU サーバを選択します。

同一機種の UTN サーバを複数台使用している場合は、特定のデバイスをデフォルト名 (⇨ 🗎65) または接続している USB デバイスで識別できます。

4. ショートカットメニューで、**IP アドレスの設定**を選択します。
   IP アドレスの設定ダイアログが表示されます。
5. 関連する TCP/IP パラメータを入力します。

6. **OK** をクリックします。

3.2 設定が保存されます。IPv6 パラメータの設定方法

IPv6 (Internet Protocol version 6) は、より一般的な IPv4 (Internet Protocol version 4) の後継バージョンです。IPv6 は以前と同様の基本機能を提供しますが、他に 2^{32} (IPv4) に代わる 2^{128} (IPv6) の拡張された IP アドレス領域や自動設定などの多くの利点があります。

重要：

IPv6 のアドレス表記は IPv4 と異なります。IPv6 アドレスは、128 ビットで構成されます。IPv6 アドレスの標準形式は、8 フィールドです。各フィールドには、16 ビットを表す 4 つの 16 進数が含まれています。

例：`2001:db8:4:0:2c0:ebff:fe0f:3b6b`

Web ブラウザで URL として使用する場合、IPv6 アドレスは角括弧で囲う必要があります。これにより、ポート番号を IPv6 アドレスの一部と間違えられることを防止できます。

例：`http://[2001:db8:4:0:2c0:ebff:fe0f:3b6b]:443`

この URL としてのアドレス形式は、IPv6 に対応するブラウザ以外は使用できません。

UTN サーバは、IPv6 ネットワークに組み込むことができます。

警告

UTN (⇨ 🗎1) と対応する SEH UTN Manager は IPv4 ネットワークでのみ機能します。

IPv6 単独のネットワークでは myUTN Control Center (⇨ 🗎6) のみが UTN サーバの管理に利用できます。

UTN サーバは、IPv4 アドレスの他に 1 つ以上の IPv6 アドレスも自動的に受信します。UTN サーバをネットワークに最適な形で組み込むために、IPv6 パラメータを設定することができます。

1. myUTN Control Center を起動します。
2. **ネットワーク – IPv6** を選択します。
3. IPv6 パラメータを設定します。⇨ 表 3 🗎18
4. **保存して再起動する**をクリックして確定します。

↳ 設定が保存されます。

表3： IPv6 パラメータ

パラメータ	説明
IPv6	UTN サーバの IPv6 機能を、有効または無効にします。
自動設定	UTN サーバへの IPv6 アドレスの自動割り当てを、有効または無効にします。
IPv6 アドレス	IPv6 ユニキャストアドレスを指定します。このアドレスは n:n:n:n:n:n:n:n の形式で UTN サーバに手動で割り当てます。 • 各「n」は、アドレスの 8 つの 16 ビット要素の 1 つの 16 進数の値を示します。 • フィールド内の先頭のゼロは省略できます。 • IPv6 アドレスは、連続するフィールドの内容がすべてゼロ (0) である場合、短縮バージョンを使用して入力または表示できます。この場合、2 つのコロン (::) を使用します。
ルータ	UTN サーバが要求を送信する宛先の静的ルータを手動で指定します。

パラメータ	説明
プレフィックス長	IPv6 アドレスのサブネットプレフィックスの長さを設定します。64 の値があらかじめ設定されています。 アドレス範囲 (ネットワークなど) は、プレフィックスを使用して指定します。指定するには、プレフィックス長 (使用するビット数) を 10 進数で IPv6 アドレスに追加し、その 10 進数の先頭にスラッシュ (/) を付けます。

3.3 WLAN を設定する方法

「myUTN-55」は、WLAN (Wireless Local Area Network) デバイスで次の規格に対応しています。

- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

myUTN Control Center では、ネットワーク – WLAN で現在の WLAN 設定を表示できます。

UTN サーバを最適な形でネットワークに組み込むには、WLAN パラメータを WLAN 設定 (ネットワーク名、暗号化、など) と一致するように設定します。そのためには、UTN サーバがすでに WLAN に組み込まれ、アドレス指定できる必要があります。初期設定については、使用する製品の ð&「クイック・インストール案内」で説明されています。

✓ WLAN の設定の知識があること。
✓ UTN サーバが WLAN 範囲内にあること。

重要：
UTN サーバは、ネットワークが変更されると、新たな IP 設定を受信します。この場合、myUTN Control Center への接続が中断します。

1. myUTN Control Center を起動します。
2. **ネットワーク** - **WLAN** を選択します。
3. WLAN パラメータを設定します。⇨ 表 4 🗎19
4. **保存して再起動する**をクリックして確定します。

↳ 設定が保存されます。

表4： WLAN パラメータ

パラメータ	説明
モード	通信モード (ネットワークインフラストラクチャ) を指定します。 • アドホック：WLAN は分散化されたアドホックネットワークで、デバイスがお互いに (ピアツーピアで) 通信します。 • インフラストラクチャ：WLAN は、アクセスポイント / ルータが中央の通信ハブとして機能するインフラストラクチャネットワークです。アクセスポイントは、固定ネットワークにケーブル接続されています。
ネットワーク名 (SSID)	SSID (Service Set Identifier) としても知られている WLAN のネットワーク名を入力します。

パラメータ	説明
ローミング	ローミング (アクセスポイント / ルータの切り替え) を、有効または無効にします。複数の (同一設定の) アクセスポイント / ルータがある広域に跨る WLAN で UTN サーバの位置を変更すると、ローミングがアクティブな場合に、UTN サーバは接続ロスのない良好な信号へと自動的に切り替わります。 (インフラストラクチャモードのみ)
チャンネル	WLAN のチャンネル (周波数範囲) を入力します。 (アドホックモードのみ)  **警告** 国から許可された WLAN チャンネルのみを使用してください。 UTN は、多くのチャンネルに対応するグローバルな製品です。一方で、チャンネルは各国の法令によって規制されています。したがって、UTN は使用する国で禁止されたチャンネルにも対応している場合があります。 国の規制には、各自が注意してください。
暗号化方式	WLAN を保護する暗号化方式を選択します。  **重要：** WEP には 16 進数キーを使用することを推奨します。 アクセスポイント / ルータによっては、ASCII フォーマットの WEP キーを 16 進数フォーマットへ変換します。この場合は、UTN サーバ上の ASCII キーとアクセスポイント / ルータ上の 16 進数が一致しません。
WEP キーを使用	使用する WEP キーを指定します。
キー 1 ～ 4	WEP キーを指定します。4 つの WEP キーが利用できます。キーの種類によって WEP キーの最大文字数と使用できる文字セットが決定されます。  **重要：** アクセスポイントが複数の WEP キーに対応する場合は、アクセスポイントのキー番号と UTN サーバが同一であることを確認してください。 例：ABCDE は、両方のデバイスで 2 つの番号を持つ必要があります (ただし、アクセスポイントが 1、UTN サーバが 2 ではありません)。
PSK	Wi-Fi Protected Access (WPA) 用の Pre Shared Key (PSK) を指定します。
認証方式	WLAN で使用している認証メカニズムを選択します。 詳細は、「ネットワーク認証を設定する方法 (IEEE 802.1X)」」⇨ 57 を参照してください。

3.4 DNS を設定する方法

DNS はドメイン名を IP アドレスに変換するサービスです。DNS を有効にしてサーバを指定する場合に、ホスト名を IP アドレスの代わりに入力できるようにします。

例：タイムサーバ設定 (⇨ 🗎27) に `10.168.0.140` の代わりに `ntp.server.de` を使用。

重要：

ネットワークが適切に設定されていると、UTN サーバは DNS 設定を DHCP により自動的に受信します。自動的に割り当てられた DNS サーバは、手動設定よりも常に優先されます。

✓ ネットワークに DNS サーバがあること。

1. myUTN Control Center を起動します。
2. **ネットワーク - DNS** を選択します。
3. DNS パラメータを設定します。⇨ 表 5 🗎21
4. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

表5： DNS パラメータ

パラメータ	説明
DNS	DNS サーバによる名前解決を、有効または無効にします。
プライマリ DNS サーバ	プライマリ DNS サーバの IP アドレスを指定します。
セカンダリ DNS サーバ	セカンダリ DNS サーバの IP アドレスを指定します。 セカンダリ DNS サーバは、プライマリ DNS サーバが利用できない場合に使用されます。
ドメイン名 (サフィックス)	既存の DNS サーバのドメイン名を指定します。

3.5 SNMP の設定方法

SNMP (Simple Network Management Protocol) は、ネットワークの構成要素を設定、監視するためのプロトコルです。このプロトコルは、監視対象デバイスと監視側装置 (SNMP 管理ツール) との間の通信を制御します。情報は読み込んで変更することができます。

SNMP には 3 つのバージョンがあり、UTN はバージョン 1 および 2 に対応しています。

SNMPv1

SNMPv1 は最初の最も単純な SNMP のバージョンです。SNMPv1 のデメリットは、コミュニティ (コミュニティグループ、監視側装置、監視対象デバイス) の不安定なアクセス制御ですが、この構成要素は容易に管理できます。コミュニティには、読み取り専用と読み取り / 書き込みの 2 種類があります。コミュニティ名はその両方で、監視側装置と監視対象デバイス間で使用されるパスワードでもあります。パスワードは平文で送信されるため、十分に保護されていません。

SNMPv3

SNMPv3 は最新の SNMP バージョンです。特長は、暗号化および認証などの拡張と新たなセキュリティです。そのために、SNMP のユーザ名と パスワードを監視側装置に対し作成する必要があります。次にこのユーザを UTN サーバ側に設定する必要があります。

重要：

また、ユーザアカウントは myUTN Control Center へのアクセスにも使用されます。**セキュリティ - デバイスへのアクセス** から指定します。「myUTN Control Center へのアクセスを保護する方法 (ユーザアカウント)」⇨ 🗎49

✓ SNMPv3 ユーザを、監視側装置に作成すること。(SNMPv3 のみ)
✓ 監視側装置の SNMPv3 ユーザが UTN サーバ ⇨ 🗎49 上に指定されていること。(SNMPv3 のみ)

1. myUTN Control Center を起動します。
2. **ネットワーク** - **SNMP** を選択します。
3. SNMP パラメータを設定します ⇨ 表 6 🗎22。
4. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

表6： SNMP パラメータ

パラメータ	説明
SNMPv1	SNMPv1 を有効または無効にします。
読み取り専用	コミュニティに対する書き込み禁止を、有効または無効にします。
コミュニティ	SNMP コミュニティ名：監視側装置に設定されている名前を入力します。 **重要：** デフォルト名は「public」です。その名前は、読み取り / 書き込みコミュニティに共通で使用されます。セキュリティの要件から、名前をできるだけ早く変更することを推奨します。
SNMPv3	SNMPv3 を有効または無効にします。
ハッシュ	ハッシュアルゴリズムを定義します。
アクセス権	SNMP ユーザのアクセス権を設定します。
暗号化	暗号化の方法を指定します。

3.6 Bonjour の設定方法

Bonjour は、TCP/IP ネットワークで自動的にデバイスやサービスを検出する技術です。
UTN サーバは Bonjour を使用して、

- IP アドレスを検証します。
- ネットワークサービスをアナウンスし検索します。
- ホスト名と IP アドレスの整合します。

1. myUTN Control Center を起動します。
2. **ネットワーク** - **Bonjour** を選択します。
3. Bonjour パラメータを設定します。⇨ 表 7 🗎22
4. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

表7： Bonjour パラメータ

パラメータ	説明
Bonjour	Bonjour を有効または無効にします。
Bonjour 名	UTN サーバの Bonjour 名を設定します。 UTN サーバは、この名前を Bonjour サービスのアナウンスに使用します。 Bonjour 名を入力しなかった場合は、デフォルト名 (デバイス名 @ICxxxxxx) が使用されます。

3.7 電子メール (POP3 と SMTP) を設定する方法

UTN サーバは電子メール (⇨ 🗎14) により管理することができ、電子メールでステータスとエラーメッセージを送信する通知サービス (⇨ 🗎29) を提供します。この機能を使用するには、電子メールプロトコルの POP3 と SMTP を UTN サーバ上にセットアップする必要があります。

UTN サーバなどのクライアントは、メールサーバから電子メールを取り込むために POP3 (Post Office Protocol Version 3) を使用します。POP3 を UTN サーバ上でセットアップし、電子メールで管理できるようにする必要があります。

SMTP (Simple Mail Transfer Protocol) を、電子メールの送信と転送のために使用します。UTN サーバは、電子メールによる管理および通知サービスのために SMTP を必要とします。

- POP3 を設定する ⇨ 🗎23
- SMTP を設定する ⇨ 🗎24

POP3 を設定する

✓ UTN サーバのユーザアカウントが POP3 サーバ上にセットアップされていること。

1. myUTN Control Center を起動します。
2. **ネットワーク** - **電子メール**を選択します。
3. POP3 パラメータを設定します。⇨ 表 8 🗎23
4. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

表8： POP3 パラメータ

パラメータ	説明
POP3	POP3 の機能を有効または無効にします。
POP3 - サーバ名	POP3 サーバを IP アドレスまたはホスト名で指定します。 ホスト名での指定は、DNS サーバが事前設定されている場合にのみ可能です。
POP3 - サーバーポート	電子メールの受信用に UTN サーバが使用するポートを指定します。 POP3 のポート番号は 110 です。SSL/TLS (パラメータ「POP3 - セキュリティ」⇨ 🗎23) のデフォルトポート番号は 995 です。必要に応じて、POP3 サーバの説明書を参照してください。
POP3 - セキュリティ	使用する認証方法を設定します。 • APOP：POP3 サーバにログオンするときにパスワードを暗号化します。 • SSL/TLS：POP3 サーバとの通信全体を暗号化します。暗号強度は、暗号化プロトコルと暗号化レベルで設定されます ⇨ 🗎48。
POP3 - メールのチェック間隔	POP3 サーバをチェックして電子メールを確認する時間間隔を分単位で指定します。
POP3 - メールサイズの上限数	UTN サーバが許容する電子メールの最大サイズを Kbyte 単位で設定します。 (0 = 無制限)
POP3 - ユーザ名	POP3 サーバにログインするために UTN サーバが使用するユーザ名を設定します。
POP3 - パスワード	POP3 サーバにログインするために UTN サーバが使用するユーザパスワードを設定します。

SMTP を設定する

✓ UTN サーバのユーザアカウントが SMTP サーバ上にセットアップされていること。

1. myUTN Control Center を起動します。
2. **ネットワーク** - **電子メール**を選択します。
3. SMTP パラメータを設定します ⇨ 表 9 🗎24。
4. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

表9： SMTP パラメータ

パラメータ	説明
SMTP - サーバ名	SMTP サーバを IP アドレスまたはホスト名で指定します。 ホスト名での指定は、DNS サーバが事前設定されている場合にのみ可能です。
SMTP - サーバーポート	UTN サーバおよび SMTP サーバが通信に使用するポートを指定します。 SMTP のデフォルトポート番号は 25 です。SSL/TLS (パラメータ 「SMTP – SSL/TLS」⇨ 🗎24) に対して、SMTP は初期値でポート 587 (STARTSSL/STARTTLS) または以前のポート 465 (SMTPS) を使用します。必要に応じて、SMTP サーバの説明書を参照してください。
SMTP – SSL/TLS	SSL/TLS を有効または無効にします。 SSL/TLS は UTN から SMTP サーバへの通信を暗号化します。暗号強度は、暗号化プロトコルと暗号化レベルで設定されます ⇨ 🗎48。
SMTP - 送信者名	UTN サーバが電子メールの送信に使用する電子メールアドレスを設定します。 多くの場合、送信者の名前と電子メールアカウントのユーザ名は同一になります。
SMTP - ログイン	SNMP の認証を有効または無効にします。電子メールを送信する場合、UTN は自己認証のために自らのユーザ名とパスワードを SMTP サーバに送信します。ユーザ名 (パラメータ 「SMTP - ユーザ名」⇨ 🗎24) およびパスワード (パラメータ 「SMTP - パスワード」⇨ 🗎24) を入力します。 SMTP サーバの中には、不正使用 (スパム) を防止するために SMTP 認証を必要とするものがあります。
SMTP - ユーザ名	SMTP サーバにログインするために UTN サーバが使用するユーザ名を設定します。
SMTP - パスワード	SMTP サーバへのログインに使用する UTN サーバのパスワードを設定します。
SMTP - セキュリティ (S/MIME)	電子メールセキュリティ規格の S/MIME (Secure/Multipurpose Internet Mail Extensions) を、有効または無効にします。S/MIME は電子メールに署名するため (「SMTP - 電子メールの署名」⇨ 🗎24) または電子メールを暗号化 (「SMTP - 完全な暗号化」⇨ 🗎24) するために使用されます。任意の機能を有効にします (「SMTP - 公開キーの添付」⇨ 🗎25)。
SMTP - 電子メールの署名	電子メールの署名を有効にします。受信者は、署名を使用して送信者の識別情報をチェックできます。署名は電子メールが改ざんされていないことを証明します。 電子メールに署名を使用するには S/MIME 証明書が必要です。⇨ 🗎52
SMTP - 完全な暗号化	電子メールの暗号化を有効にします。暗号化された電子メールは、対象の受信者のみが開いて読むことができます。 暗号化には S/MIME 証明書が必要です ⇨ 🗎52。

パラメータ	説明
SMTP - 公開キーの添付	公開キーを電子メールと一緒に送信します。 多くの電子メールクライアントが、電子メールを表示するキーを必要とします。

3.8 VLAN 環境での UTN サーバの利用方法 (myUTN-80 以降のみ)

UTN サーバは、802.1Q に従い VLAN (Virtual Local Area Network) に対応しています。

VLAN は、物理ネットワークを論理的なサブネットワークに分割します。各サブネットワークは自らのブロードキャストドメインを持つため、サブネットワーク間でのデータパケットの交換はできません。VLAN は構築されたネットワークのセキュリティを強化するために使用されます。

各 USB デバイスは VLAN に割り当てることができます。VLAN データを USB ポート経由で転送するには、最初に VLAN を UTN サーバに入力する必要があります。次に、データ転送に使用する USB ポートを指定した VLAN にリンクする必要があります。

USB デバイスへのアクセスは、特に VLAN を使用すると調整することができます。例えば、ネットワークユーザのうち指定したグループのみが特定の USB デバイスを使用するようにできます。
VLAN をユーザの環境に実装する方法を確認した上で、UTN サーバをセットアップしてください。

- IPv4 管理 VLAN を設定する ⇨ 🗎25
- IPv4 クライアント VLAN を設定する ⇨ 🗎26
- USB ポートに IPv4 クライアント VLAN を割り当てる ⇨ 🗎26

IPv4 管理 VLAN を設定する

1. myUTN Control Center を起動します。
2. **ネットワーク** - **IPv4 VLAN** を選択します。
3. IPv4 VLAN パラメータを設定します。⇨ 表 10 🗎25
4. 確定するには、**保存**をクリックします。
5. 設定が保存されます。

表10：IPv4 管理 VLAN パラメータ

パラメータ	説明
IPv4 管理 VLAN	IPv4 管理 VLAN データの転送を、有効または無効にします。 この設定を有効にした場合、SNMP は IPv4 管理 VLAN でのみ利用できます。
VLAN ID	IPv4 管理 VLAN を識別するための ID (0 ～ 4096) です。
IP アドレス	UTN サーバの IP アドレスです ⇨ 🗎16。
サブネットマスク	UTN サーバのサブネットマスクです ⇨ 🗎16。
ゲートウェイ	UTN サーバが使用しているネットワークの標準ゲートウェイの IP アドレスです ⇨ 🗎16。 ゲートウェイにより、外部ネットワークから IP アドレスを指定できます。
任意の VLAN からのアクセス	IPv4 クライアント VLAN を介した UTN サーバへの管理者アクセス (Web) を、有効または無効にします。 この設定が有効な場合、UTN サーバはすべての VLAN を介して管理できます。

パラメータ	説明
LAN からのアクセス (タグなし)	タグなしの IPv4 パケットを介した UTN サーバへの管理者アクセスを、有効または無効にします。 この設定が無効な場合、UTN サーバは VLAN を介してのみ管理できます。

IPv4 クライアント VLAN を設定する

1. myUTN Control Center を起動します。
2. **ネットワーク** - **IPv4 VLAN** を選択します。
3. IPv4 VLAN パラメータを設定します。⇨ 表 11 🗎26
4. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

表11：IPv4 クライアント VLAN パラメータ

パラメータ	説明
VLAN	IPv4 クライアント VLAN データの転送を、有効または無効にします。
IP アドレス	IPv4 クライアント VLAN 内にある UTN サーバの IP アドレスです。
サブネットマスク	IPv4 クライアント VLAN 内にある UTN サーバのサブネットマスクです。
ゲートウェイ	IPv4 クライアント VLAN のゲートウェイアドレスです。
VLAN ID	IPv4 クライアント VLAN を識別するための ID (0 ～ 4096) です。

Auto-fll を使用して、VLAN、IP アドレスおよびサブネットマスクをその値でライン 1 から自動的に埋めます。VLAN ID は 1 つずつカウントアップされます。

USB ポートに IPv4 クライアント VLAN を割り当てる

1. myUTN Control Center を起動します。
2. **セキュリティ** - **USB ポートアクセス**を選択します。
3. **VLAN の割り当て**リストから、VLAN を USB ポートに割り当てます。
4. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

4 デバイス設定

4.1 デバイス時間の設定方法

UTN サーバのデバイス時間は、ネットワーク上の SNTP タイムサーバ (簡易ネットワーク時刻プロトコル) により設定できます。タイムサーバは、ネットワーク内のデバイスの時間を同期します。

今日優先される時刻標準として「UTC」(協定世界時) が使用されています。地域に応じてタイムゾーンで補正されます。

重要：

適切に設定されたネットワーク上で、UTN サーバはタイムサーバ設定を DHCP により自動的に受信します。自動的に割り当てられたタイムサーバは、手動で設定されたタイムサーバより常に優先されます。

✓ ネットワークにタイムサーバがあること。

1. myUTN Control Center を起動します。
2. **デバイス** - **日付 / 時間**を選択します。
3. **日付 / 時間**にチェックマークを付けます。
4. **タイムサーバ**欄に、タイムサーバの IP アドレスまたはホスト名を入力します。
   (ホスト名が指定できるのは、DNS サーバがあらかじめ設定されている場合にのみです。⇨ 🗎21)
5. **タイムゾーン**リストから、ローカルのタイムゾーンのコードを選択します。
6. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

4.2 説明の記述内容を設定する方法

UTN サーバには、任意の説明を割り当てることができます。これにより、ネットワーク内で利用できるデバイスの概要がわかりやすくなります。

また、USB ポートを識別するために名前を割り当てることができます。
⇨ 🗎28

1. myUTN Control Center を起動します。
2. **デバイス** - **説明**を選択します。
3. **ホスト名**、**説明**および**担当者**の任意の名前を入力します。
4. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

表12：解説

パラメータ	説明
ホスト名	IP アドレスに代わるデバイス名。名前により、例えば複数の UTN サーバを使用している場合、ネットワーク上で UTN サーバを容易に識別できます。 myUTN Control Center および SEH UTN Manager に表示されます。
説明	場所や所属部門などのデバイスの説明。 myUTN Control Center および SEH UTN Manager に表示されます。
担当者	デバイス管理者などの担当者。 myUTN Control Center に表示されます。

4.3 USB ポートに名前を割り当てる方法

初期設定で、接続された USB デバイスの名前は myUTNControl Center と SEH UTN Manager の USB ポートに表示されます。デバイスメーカが設定した名前は、曖昧で不正確な場合があります。

この理由から、例えば対応するソフトウェア名のような自由に設定できる名前を USB ポートに割り当てることができます。そのような名前を付けることで、ネットワーク内で使用できる USB デバイスの概要が理解しやすくなります。

1. myUTN Control Center を起動します。
2. **デバイス** - **USB ポート**を選択します。
3. **ポート名**欄に任意の名前を入力します。
4. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

4.4 USB ポートを無効にする方法 (myUTN-80 以降のみ)

初期設定では、すべての USB ポートがアクティブです。USB ポートを、電源を遮断または再確立することで非アクティブ化 (再度アクティブ化) にすることができます。

非アクティブ化

- 不要な USB デバイスがネットワークに接続できないようにするために、使用していない USB ポートを非アクティブにします。(非アクティブ状態の USB ポートは、SEH UTN Manager で表示されません。)
- USB ポートを非アクティブにして再度アクティブ化することで、不定な状態の接続された USB デバイスを再起動します。(USB デバイスを手作業で取り外して再接続する必要がありません。)

1. myUTN Control Center を起動します。
2. **デバイス** - **USB ポート**を選択します。
3. **USB ポート**の前のオプションにチェックマークを付ける、またはチェックマークを外します。
4. 確定するには、**保存**をクリックします。

↳ USB ポートが、無効または有効になります。

4.5 UTN (SSL) ポートの設定方法

UTN サーバ (接続された USB デバイスを含む) とクライアント間のデータ転送に、共有ポートを使用します。ポートは接続の種類に依存します。

- 暗号化されていない USB 接続：UTN ポート (デフォルト：9200)
- 暗号化された USB 接続 (⇨ 🗎46)：UTN SSL ポート (デフォルト：9443)

警告

UTN ポートや UTN SSL ポートは、セキュリティ対策 (ファイアウォール) で遮断しないでください。

例えばポート番号がネットワーク上の他のアプリケーションですでに使用されている場合、ポート番号を変えることができます。変更は UTN サーバ上で実行し、クライアントにインストールされた SEH UTN Manager に SNMPv1 でリレーされます。

✓ SNMPv1 が有効なこと。⇨ 🗎21

1. myUTN Control Center を起動します。
2. **デバイス** - **UTN ポート**を選択します。
3. **UTN ポート**、または **UTN SSL ポート**欄にポート番号を入力します。
4. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

4.6 メッセージを取得する方法 (myUTN-80 以降のみ)

UTN サーバは次のような様々な メッセージを送信することができます。

- ステータス通知：UTN サーバや接続された USB デバイスの状態を通知する電子メールを定期的に送信します。
- 電子メールまたは SNMP トラップによるイベント通知
  - USB デバイスが UTN サーバに接続されている /UTN サーバから切断されている
  - USB ポート (接続された USB デバイスへの接続など) が、アクティブ化または非アクティブ化されている。
  - UTN サーバの再起動
  - 電源が遮断または再確立されている (myUTN-800 のみ)
  - ネットワーク接続が遮断または再確立されている (myUTN-800 のみ)
  - SD カードが UTN サーバに挿入されている / UTN サーバから取り外されている (myUTN-800 のみ)
  - SC カードが使用できない (myUTN-800 のみ)

- ステータス通知の送信を設定する ⇨ 🗎29
- 電子メールでのイベント通知を設定する ⇨ 🗎30
- SNMP トラップでのイベント通知を設定する ⇨ 🗎30

ステータス通知の送信を設定する

ステータス通知は、最大 2 人の受信者に送信できます。

✓ SMTP がセットアップされていること。⇨ 🗎23

✓ DNS がセットアップされていること。⇨ 🗎21

1. myUTN Control Center を起動します。
2. **デバイス** - **通知**を選択します。
3. **電子メールアドレス**欄に受信者を入力します。

4. **ステータス通知**領域の受信者にチェックマークを付けます。
5. 間隔を設定します。
6. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

電子メールでのイベント通知を設定する

イベント通知は、最大 2 人の受信者に送信できます。

✓ SMTP がセットアップされていること。⇨ 🗎23

✓ DNS がセットアップされていること ⇨ 🗎21。

1. myUTN Control Center を起動します。
2. **デバイス** - **通知**を選択します。
3. **電子メールアドレス**欄に受信者を入力します。
4. メッセージタイプのオプションに、チェックマークを付けます。
5. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

SNMP トラップでのイベント通知を設定する

イベント SNMP トラップは、最大 2 人の受信者に送信できます。

✓ SNMPv1 または / および SNMPv3 がセットアップされていること。⇨ 🗎21

1. myUTN Control Center を起動します。
2. **デバイス** - **通知**を選択します。
3. **SNMP トラップ**の領域で、受信者を IP アドレスとコミュニティにより設定します。
4. メッセージタイプのオプションに、チェックマークを付けます。
5. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

4.7 音響信号の設定方法 (myUTN-800 のみ)

myUTN-800 Dongleserver は、次の場合に音によるフィードバックを返します。

- USB ドングルが接続されたとき
- Dongleserver の再起動
- パラメータがリセットされたとき

音響信号はオフにできません。

さらに任意で、次のイベントに対する音響フィードバックを設定できます。

- 1 個の電源だけが動作
- SD カードのエラー (読み取り / 書き込みエラー、SD カードなし)
- 1 つのネットワーク接続のみが確立されてるとき

このオプションの音響信号は、ディスプレイパネル上のエラーメッセージを完全に補完します ⇨ 🗎31。

1. myUTN Control Center を起動します。
2. **デバイス** - **通知**を選択します。
3. **音響信号**領域で、任意のメッセージタイプのオプションにチェックマークを付けます。
4. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

4.8 ディスプレイに表示する項目を決定する方法 (myUTN-800 のみ)

Dongleserver myUTN-800 は、前面にディスプレイパネルが装備され、次の情報を表示できます。

- 識別子：任意に設定できる名前で初期値で表示されます。初期値：DS)
- エラー状態：次のイベントが発生したときに表示できる任意の通知：
  - 1 個の電源だけが動作
  - SD カードのエラー (読み取り / 書き込みエラー、SD カードなし)
  - 1 つのネットワーク接続のみが確立されてるとき

  エラーはコードで表示されます。

  表13：エラーコード

テキスト	説明	トラブルシューティング
DS (各識別子)	Dongleserver が使用できます。	–
RS	Dongleserver が再起動します。	–
DL	Dongleserver にファームウェア / ソフトウェアが読み込まれます。その後、Dongleserver が更新されます。	–
E1	2 つの電源のうち 1 つが動作していません。 アクティブでない接続は、ドットの点灯で示されます。(左のドット、左の電源、右のドット、右の電源)	ケーブル接続と電圧源を確認します。
E2	サポート外のファイルシステムでフォーマットされた SD カードは、読み書きができません。	• SD カードを FAT32、FAT16、または FAT12 のファイルシステムでフォーマットします。 • SD カードが正確に機能していることを確認します。
E3	この SD カードは読み取り専用です。	SD カードの書き込み禁止を解除します。
E4	カードリーダに利用できる SD カードがありません。	SD カードを SD カードリーダに挿入します。 • 種類：SD または SDHC • ファイルシステム FAT32、FAT16、または FAT12
E5	両方のネットワーク接続の一方にリンクがありません。	ケーブル接続とネットワークを確認します。

- 識別子を設定する ⇨ 31
- エラー通知を有効にする ⇨ 32

識別子を設定する

複数の myUTN-800 が 1 つのサーバラック、または同じ場所に設置されているときに、デバイスを識別するための識別子を使用します。

1. myUTN Control Center を起動します。
2. **デバイス** - **説明**を選択します。
3. 任意の説明を **識別子 (ディスプレイパネル)** 欄に入力します。
   (最大 2 半角文字；A ～ Z、0 ～ 9)E+ 数字の組合せは、エラーに使用するため指定できません。

4. 確定するには、**保存**をクリックします。
↳ 設定が保存されます。

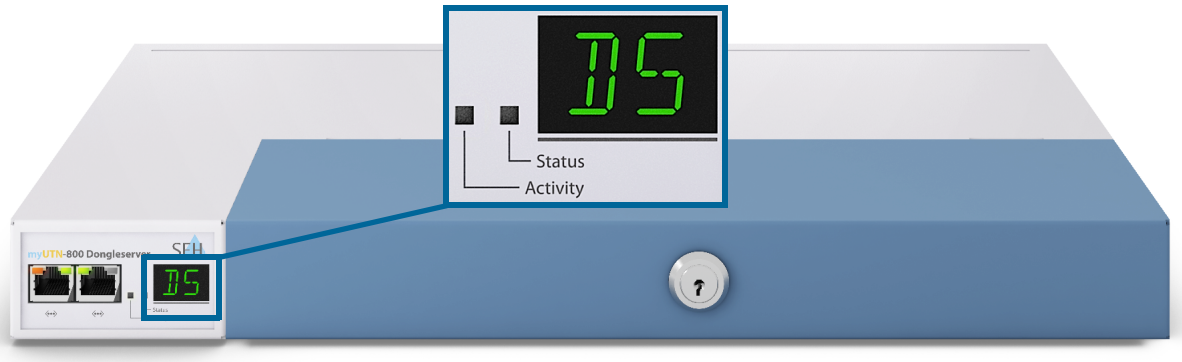


図 3： ディスプレイパネル myUTN-800

エラー通知を有効にする

1. myUTN Control Center を起動します。
2. **デバイス** - **通知**を選択します。
3. **ディスプイパネル**領域で、メッセージタイプのオプションにチェックマークを付けます。
4. 確定するには、**保存**をクリックします。
↳ 設定が保存されます。

オプションの音響信号は、ディスプレイパネル上のエラーメッセージを完全に補完します。⇨ 🗎30

5 SEH UTN Manager の操作

「SEH UTN Manager」は、SEH Computertechnik GmbH が開発したソフトウェアツールです。SEH UTN Manager は、UTN サーバに接続された USB デバイスへの接続を確立し管理するために使用されます。

5.1 ネットワーク内の UTN サーバと USB デバイスを検索する方法

SEH UTN Manager ソフトウェアツールは、UTN サーバに接続された USB デバイスへの接続を確立し管理するために使用されます。

SEH UTN Manager を起動すると、ネットワークをスキャンして、接続された UTN サーバを検出します。スキャンするネットワーク範囲は任意に設定できます。検索はマルチキャストや設定可能な IP 範囲から実行できます。初期値は、ローカルネットワークセグメント内でのマルチキャスト検索に設定されています。

検出されたすべての UTN サーバとそのサーバに接続された USB デバイスが「ネットワークリスト」に表示されます。UTN サーバに接続された USB デバイスを使用するには、UTN サーバを「選択リスト」に追加します。

UTN サーバを直接選択リストに追加することもできます。これを実行するには、サーバの IP アドレスが分かっていなければなりません。

検索パラメータを設定する

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 🗎8

1. SEH UTN Manager を起動します。
2. メニューバーから、プログラム – オプションを選択します。
   オプションダイアログが表示されます。
3. ネットワークスキャンタブを選択します。
4. IP 範囲検索にチェックマークを付け、少なくとも 1 つのネットワーク範囲を指定します。
5. OK をクリックします。

↳ 設定が保存されます。

ネットワークをスキャンする

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 8

1. SEH UTN Manager を起動します。
2. メニューバーから、選択リスト – 編集を選択します。
   選択リストの編集ダイアログが表示されます。
3. スキャンをクリックします。
4. ネットワークがスキャンされます。検出された UTN サーバと USB デバイスが、ネットワークリストに表示されます。

UTN サーバを選択リストに追加する

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 8
✓ UTN サーバがネットワークスキャンで検出され、ネットワークリストに表示されていること。

1. SEH UTN Manager を起動します。
2. メニューバーから、選択リスト – 編集を選択します。
   選択リストの編集ダイアログが表示されます。
3. 選択リストから使用する UTN サーバを選択します。
4. 追加をクリックします。
   (必要に応じて、2 と 3 の手順を繰り返し実行します。)
5. OK をクリックします。

↳ UTN サーバおよび接続された USB デバイスが、選択リストに表示されます。

図 4： SEH UTN Manager - 選択リストの編集

UTN サーバを IP アドレスにより追加する

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 8
✓ UTN サーバの IP アドレスが分かっていること。

1. SEH UTN Manager を起動します。
2. UTN サーバ – 追加を選択します。
   サーバの追加ダイアログが表示されます。
3. **ホスト名または IP アドレス**の欄に、UTN サーバの IP アドレスを入力します。
4. UTN ポートや UTN SSL ポート (⇨ 29) を変更した場合は、**UTN- ポート**と **UTN-SSL- ポート**欄に各ポート番号を設定してください。
5. OK をクリックします。

↳ UTN サーバおよび接続された USB デバイスが、選択リストに表示されます。

5.2 USB デバイスへの接続を確立する方法

USB デバイスをクライアントに接続する場合は、クライアントと USB デバイスが接続された UTN サーバの USB ポート間のポイントツーポイント接続を確立します。クライアントは、UTN サーバに接続された USB デバイスを、直接クライアントに接続された USB デバイスと同じ感覚で使用できます。

重要：

複合 USB デバイスの特殊なケース

特定のタイプの USB デバイスを UTN サーバの USB ポートに接続すると、選択リストはそのポートに複数の USB デバイスを表示します。このタイプのデバイスは、複合 USB デバイスです。ハブと 1 台以上の USB デバイスから構成され、すべて 1 つのハウジングに組み込まれています。

複合 USB デバイスが接続されたポートへの接続が確立すると、表示される USB デバイスはすべてそのユーザのクライアントに接続されます。この場合、組み込まれた各 USB デバイスは、UTN サーバの 仮想 USB ポートを使用します。仮想 USB ポートの数が制限され、ポート数は UTN サーバの機種により異なります。制限数に達すると、その UTN サーバでそれ以上の USB デバイスを使用することができません。

UTN サーバ	仮想 USB ポート数	UTN サーバ	仮想 USB ポート数
myUTN-50a	6	myUTN-800	40
myUTN-55	6	myUTN-2500	12
myUTN-80	16		

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 8
✓ USB ポートが選択リスト上に表示されていること。⇨ 33
✓ クライアント側は、USB デバイスをローカルで操作する (直接クライアントに接続する) ために必要な条件 (ドライバのインストールなど) がすべて満たされていること。対象の USB デバイスをメーカの説明書に従って実際にローカルでクライアントに接続し、動作を確認することを推奨します。
✓ USB ポートが、別のクライアントに接続されていないこと。

1. SEH UTN Manager を起動します。
2. 選択リストからポートを選択します。
3. メニューバーから、ポート – 有効化 を選択します。

↳ USB デバイスとクライアント間の接続が確立されます。

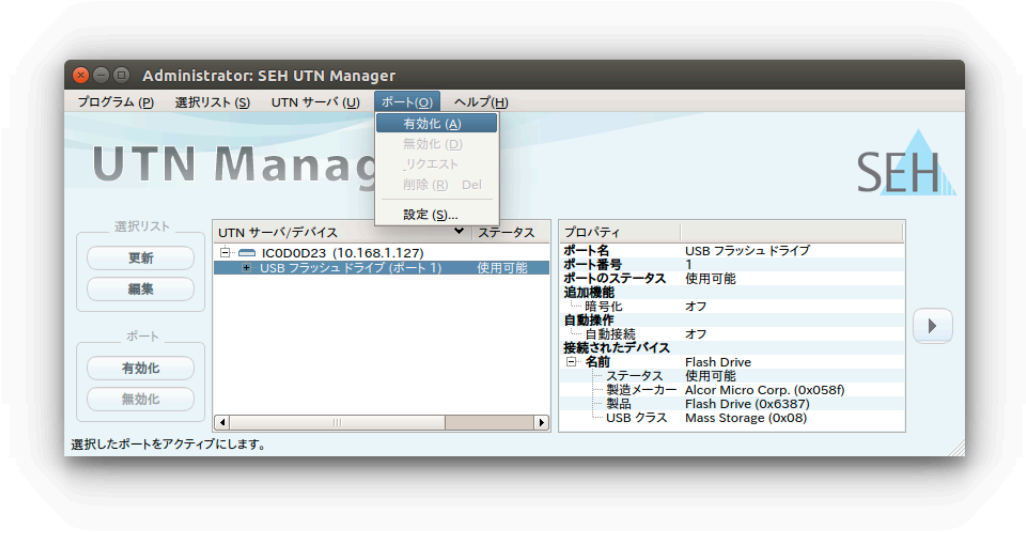


図 5： SEH UTN Manager – USB ポートのアクティブ化

5.3 USB デバイスとクライアント間の接続を解除する方法

USB デバイスがクライアントに接続されている場合、その接続タイプはポイントツーポイントです。接続が確立されている間、その USB デバイスは他のクライアントに接続することができないため、他のユーザは使用できません。そのため、使用しなくなった USB デバイスへの接続はすぐに解除する必要があります。

USB デバイスとクライアント間の接続を解除するには、クライアントと USB デバイスが接続している UTN サーバの USB ポート間の接続を非アクティブにします。

- 通常は、ユーザが SEH UTN Manager で接続を解除します。⇨ 🗎36
- また、管理者が myUTN Control Center から接続を非アクティブ化することもできます。⇨ 🗎36
- 自動的な非アクティブ化 (自動切断) をセットアップすることもできます。⇨ 🗎38

SEH UTN Manager でデバイスの接続を解除する

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 🗎8
✓ USB ポートが選択リスト上に表示されていること。⇨ 🗎33
✓ USB ポートが、クライアントに接続されていること。⇨ 🗎35

1. SEH UTN Manager を起動します。
2. 選択リストからポートを選択します。
3. メニューバーから、**ポート** - **無効化**を選択します。

↳ 接続が解除されます。

myUTN Control Center からデバイスの接続を解除する

✓ USB ポートが、クライアントに接続されていること。⇨ 🗎35

1. myUTN Control Center を起動します。
2. **ホーム**を選択します。
3. **接続済みデバイス**リストから、アクティブな接続を選択し ⊗ アイコンをクリックします。
4. セキュリティクエリを確認します。

↳ 接続が解除されます。

5.4 使用中の USB デバイスをリクエストする方法

USB デバイスがクライアントに接続されている場合、その接続タイプはポイントツーポイントです。接続が確立されている間、その USB デバイスは他のクライアントに接続することができないため、他のユーザは使用できません。

使用中の USB デバイスを使用する場合は、リクエストすることができます。他のユーザはその開放リクエストをポップアップウィンドウで受信します。ユーザがリクエストに応じて、USB デバイスへの接続を非アクティブにして開放すると、リクエストしたクライアントと USB デバイス間の接続がアクティブになります。

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 🗎8
✓ SEH UTN Manager (フルバージョン) が、USB デバイスを使用するユーザのクライアントにインストールされていること。⇨ 🗎8
✓ SEH UTN Manager (グラフィカルユーザインターフェイス付きのフルバージョン) が双方のクライアントで実行されていること。
✓ USB ポートが選択リスト上に表示されていること。⇨ 🗎33
✓ USB ポートが別のユーザに接続されていること。⇨ 🗎35 (ただし、自動接続でない状態。)

1. 選択リストからポートを選択します。
2. メニューバーから、**ポート – リクエスト** を選択します。

↳ 開放リクエストが送信されます。

5.5 USB デバイス接続とプログラムの開始を自動化する方法

UTN サーバの USB ポートと接続された USB デバイスへの接続は自動化することができます。これにより、複雑な作業が単純化されます。

- USB デバイスが接続されているときの自動的な接続 (自動接続) ⇨ 🗎37
- 設定時間後に接続を自動的に非アクティブ化 (自動切断) ⇨ 🗎38

この章では、自動操作のセットアップに使用する SEH UTN Manager の機能について説明します。スクリプトに関する専門知識がある場合は、「utnm」ツールの使用を推奨します。⇨ 🗎42

USB デバイスが接続されているときの自動的な接続 (自動接続)

自動接続は、USB デバイスが USB ポートに接続されるとすぐに、自動的に USB ポートと接続された USB デバイスへの接続を確立します。自動接続は、各 USB ポートと USB ポートに接続されたすべての USB デバイスに対する操作がアクティブにできなければなりません。

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 🗎8
✓ USB ポートが選択リスト上に表示されていること。⇨ 🗎33
✓ クライアントに管理者としてログオンしていること。

1. SEH UTN Manager を起動します。
2. 選択リストから UTN サーバを選択します。
3. メニューバーから、**UTN サーバ – 自動接続を有効化**を選択します。
   自動接続を有効化ダイアログが表示されます。
4. 対象の USB ポートにチェックマークを付けます。
5. **OK** をクリックします。

↳ 設定が保存されます。USB ポートと接続された USB デバイスへの接続が自動的にすぐにアクティブになります。USB デバイスを切断して再接続すると、再び接続が自動的に確立されます。

重要：
自動接続によりアクティブ化され確立した USB ポート接続を手動で非アクティブにすると、自動接続の設定も非アクティブになります。自動接続を再び使用するには、再度設定する必要があります。

設定時間後に接続を自動的に非アクティブ化 (自動切断)

自動切断は、事前に設定した時間が経過すると USB ポートと接続された USB デバイスへの接続を非アクティブにします。時間切れの 2 分前に、データ損失とエラー状態を防止するために、ユーザは接続の非アクティブ化を要請する通知を受信します。任意で、設定した時間内に 1 回のみ接続の延長をアクティブに設定することができます。この場合、ユーザは表示された通知のポップアップで、接続の延長を選択または拒否することができます。

自動切断機能は、多くのネットワーク参加者が限られた数のデバイスを利用できるようにし、アイドル時間を削減します。

接続が自動的に切断されポートが開放されると通知を受信することができます。そのためには、USB ポートが利用可能になった通知の設定もしてください。⇨ 🗎38

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 🗎8
✓ UTN サーバが「デバイスの自動切断」領域に表示されていること。⇨ 🗎33
✓ クライアントに管理者としてログオンしていること。

1. SEH UTN Manager を起動します。
2. メニューバーから、**プログラム – オプション**を選択します。
   オプションダイアログが表示されます。
3. **自動操作**タブを選択します。
4. **自動切断**領域で、該当する UTN サーバの**ステータス**にチェックマークを付けます。
5. 時間範囲 (10 ～ -9999 分) を設定します。
6. 任意で**延長**にチェックマークを付けます。
7. **OK** をクリックします。

↳ 設定が保存されます。

5.6 USB ポートと USB デバイスのステータス情報を検索する方法

USB ポートと USB デバイスのステータスは、いつでも確認できます。自動メッセージを設定することもできます。USB ポートが利用可能になった場合や接続時間に関する情報を受信する場合などに、自動メッセージの通知を使用することができます。

重要：
自動メッセージは表示されない場合があります。
メッセージの表示は、システムのウィンドウマネージャに依存します。
Linux システム (またウィンドウマネージャ) には数多くの種類があるため、メッセージ通知に対応していない種類もあります。

- ステータス情報を表示する ⇨ 🗎39
- USB ポートが利用可能になった場合の通知 ⇨ 🗎39
- 接続時間に関するメッセージ ⇨ 🗎39

ステータス情報を表示する

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 🗎8
✓ USB ポートが選択リスト上に表示されていること。⇨ 🗎33

1. SEH UTN Manager を起動します。
2. 選択リストから USB ポートを選択します。

↳ ステータス情報が**プロパティ**領域に表示されます。

USB ポートが利用可能になった場合の通知

ネットワーク参加者が USB ポートと接続された USB デバイスへの接続を非アクティブ化すると、メッセージを受信します。

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 🗎8
✓ USB ポートが選択リスト上に表示されていること。⇨ 🗎33

1. 選択リストからポートを選択します。
2. メニューバーから、**ポート** – **設定**を選択します。
   ポート設定ダイアログが表示されます。
3. **メッセージ**の下のオプションにチェックマークを付けます。
4. **OK** をクリックします。

↳ 設定が保存されます。

接続時間に関するメッセージ

USB ポートと接続された USB デバイスへの接続の 1 つが設定された時間を超過すると、メッセージを受信します。

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 🗎8

1. メニューバーから、**プログラム** – **オプション**を選択します。
   オプションダイアログが表示されます。
2. **プログラム**タブを選択します。
3. **メッセージ**領域で、オプションにチェックマークを付けます。
4. 任意の時間を設定します。
5. **OK** をクリックします。

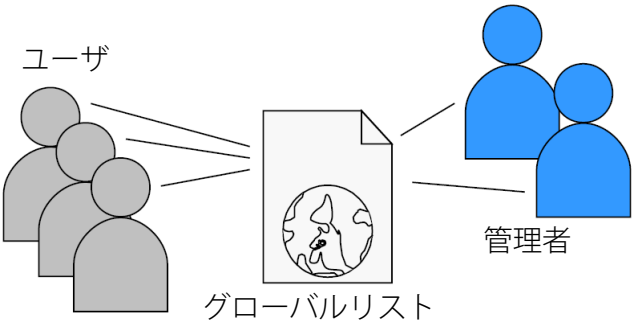
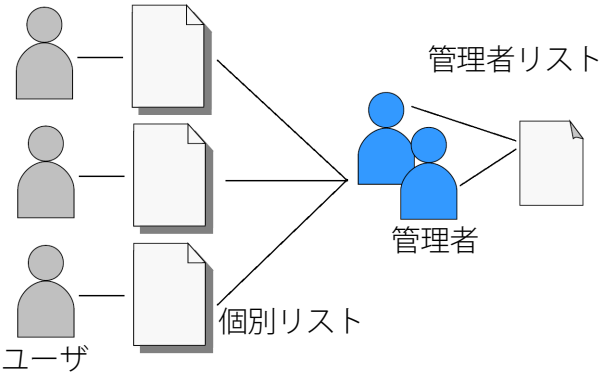
↳ 設定が保存されます。

5.7 選択リストを使用してユーザのアクセス権を管理する方法

選択リストは、SEH UTN Manager の主要な要素で、組み込まれたすべての UTN サーバを表示します。USB デバイスは、それが接続している UTN サーバが選択リスト上にある場合のみに使用できます。(⇨ 🗎33) 選択リストを制御することで、結果的に UTN サーバと接続された USB デバイスへのユーザアクセスを制御できます。

初期値では、すべてのクライアントユーザが SEH UTN Manager のグローバル選択リストを使用しますが、クライアントユーザに対してユーザ固有の選択リストを設定することができます。そのリストはユーザが任意に編集ができます。または、クライアント管理者がユーザ権限を制限して、設定した UTN サーバのみを使用できるリストを提供することも可能です。

表14：グローバルとユーザ選択リストとの相違点

グローバル選択リスト	ユーザ選択リスト
	
• 1 つのクライアントのすべてのユーザが、同じ選択リストを使用します。	• 各ユーザは、自分専用の選択リストを所有します。 すべての管理者は同じ選択リストを所有します。
• ユーザは、選択リストに表示されたすべてのデバイスにアクセスできます。 (ただし、myUTN Control Center でセキュリティメカニズムが指定されていない場合に限定されます。)	• ユーザは、選択リストに表示されたすべてのデバイスにアクセスできます。 (ただし、myUTN Control Center でセキュリティメカニズムが指定されていない場合に限定されます。)

• リストの保存場所：/etc	• リスト (「ini」- ファイル) の保存場所：
	`$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`
	(`$HOME` は Linux のユーザフォルダ用の環境変数です。現在のユーザのパスは次のコマンドラインで決定できます：`echo $HOME`
	例 Ubuntu 20.0.4.0 LTS:
	`echo $HOME` は
	`/Users home/User name` を与えます
	+
	`.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`
	ini ファイルのフルパス：
	`/Usershome/User name/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini`)

• 選択リストは、管理者が編集できます。	• 選択リストは、管理者または書き込み権限のあるユーザが編集できます。 ini- ファイルに対し読み取り専用の権限のみユーザは、選択リストを編集できず、SEH UTN Managers へのアクセスも制限されます。

SEH UTN Manager で使用できる機能 (選択リスト編集など) は、選択リストの種類 (グローバルまたはユーザ) とクライアント上のユーザアカウントの種類 (管理者 / ユーザ、ini- ファイルへの書き込み権限がある / ないユーザ) に依存します。分類の詳細は、「SEH UTN Manager – 機能の概要」⇨ 93 を参照してください。

- すべてのユーザにグローバル選択リストをセットアップする ⇨ 🗎41
- ユーザ選択リストを提供する ⇨ 🗎41
- 「SEH UTN Manager.ini」- ファイルへの書き込み権限を制限する ⇨ 🗎41

すべてのユーザにグローバル選択リストをセットアップする

初期値ではグローバル選択リストが使用されます。

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 🗎8
✓ システムに管理者としてログオンしていること。

1. SEH UTN Manager を起動します。
2. 選択リストを構成します。⇨ 🗎33
3. メニューバーから、**プログラム – オプション**を選択します。
   オプションダイアログが表示されます。
4. **選択リスト**タブを選択します。
5. **グローバル選択リスト**にチェックマークを付けます。
6. **OK** をクリックします。

↳ 設定が保存されます。1 つのクライアントのすべてのユーザが、同じ選択リストを使用します。

ユーザ選択リストを提供する

✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇨ 🗎8
✓ システムに管理者としてログオンしていること。

1. SEH UTN Manager を起動します。
2. メニューバーから、プログラム – オプションを選択します。
   オプションダイアログが表示されます。
3. 選択リストタブを選択します。
4. ユーザ選択リストにチェックマークを付けます。
5. OK をクリックします。

オプション：次の手順で所定の選択リストを提供します。

6. 対象のデバイスを含む選択リストを作成します。⇨ 🗎33
7. メニューバーから、**選択リスト – エクスポート**を選択します。
   エクスポート先ダイアログが表示されます。
8. 「SEH UTN Manager.ini」を、次のユーザディレクトリに保存します。
   $HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini (⇨ 表 14 🗎40)

↳ 設定が保存されます。各ユーザは、個別の (所定の) 選択リストを使用します。管理者は、1 つの選択リストを共有します。

「SEH UTN Manager.ini」- ファイルへの書き込み権限を制限する

ユーザ選択リストは、ユーザ自身がセットアップし編集することができます。

UTN サーバへのユーザアクセスを制限して、リストをユーザに提供することもできます。これを実行するには、管理者はユーザ (⇨ 🗎41) に対する所定のリストを保存して、「SEH UTN Manager.ini」- ファイルへのユーザアクセスを読み取り専用に制限します。ユーザ権限を読み取り専用に制限することで、選択リストに関するすべての SEH UTN Manager 機能が、対象のユーザに対して無効になります。

オペレーティングシステムの通常の方法で、ini- ファイルを読み取り専用ファイルにします。詳細は、オペレーティングシステムの説明書を参照してください。

5.8 SEH UTN Manager をグラフィカルユーザインターフェイスなしで使用する方法 (utnm)

SEH UTN Manager には 2 つのバージョンがあります。⇨ 🗎8 ミニマルバージョンでは、グラフィカルユーザインターフェイスなしで使用できます。これを実行するには、オペレーティングシステムのコンソールから「utnm」ツールを利用して UTN 機能を使用します：

- 直接。コマンドを特定の構文で入力して実行
- 特定構文のコマンドを含むスクリプト。コマンドラインインタープリタにより自動的に順次実行

スクリプトを使用して、ポートのアクティブ化のような頻繁に使用するコマンドシーケンスを自動化します。

ログインスクリプトなどを使用し、スクリプトの実行を自動化することができます。

- 構文 ⇨ 🗎42
- コマンド ⇨ 🗎42
- リターン情報 ⇨ 🗎44
- コンソールから utnm を使用する ⇨ 🗎45
- utnm スクリプトを作成する ⇨ 🗎45

構文

`utnm -c "` コマンド文字列 `" [-<` コマンド `>]`

実行ファイル「utnm」は、`/usr/bin/` にあります。

コマンド

コマンドの規則

- 未定義の要素は、適切な値 (例：サーバ = UTN サーバの IP　アドレスまたはホスト名) で置換されます。
- 角括弧内の要素は任意です。
- 大文字、小文字を区別しません。
- ASCII フォーマットのみ読み込み可能です。

コマンド	説明
-c "コマンド文字列" または --command "コマンド文字列"	コマンドを実行します。コマンドは、コマンド文字列で詳しく指定します。コマンド文字列： • activate サーバポート番号 USB ポートと接続された USB デバイスへの接続をアクティブにします。 • activate サーバ ベンダ ID (VID) 製品 ID (PID) 複数の同じ USB デバイスが UTN サーバに接続されている場合に、USB ポートと最初に接続された USB デバイスを設定された ID でアクティブにします。 • deactivate サーバポート番号 USB ポートと接続された USB デバイスへの接続を非アクティブにします。 • set autoconnect = true|false サーバポート番号 USB ポートへの自動接続 (⇨ 🗎37) を、有効または無効にします。 • set portkey='port key' サーバポート番号 USB のポートキー (⇨ 🗎51) をシステム上にローカルで保存します。このように、USB ポートキーは常に自動的に送信されるため、毎回コマンドで指定する必要がありません。-k USB ポートキー または --key USB ポートキー (次を参照)。 (USB ポートキーを削除するために使用するコマンド文字列：set portkey= サーバポート番号) **重要：** このコマンドは、USB デバイスを利用できる目的のみで、キーを正式に設定します。 USB ポートキーは、myUTNControl Center ⇨ 🗎51 で設定します。 • find ネットワークセグメント内のすべての UTN サーバを検索して、検出した UTN サーバをその IP アドレス、MAC アドレス、機種、およびソフトウェアバージョンとともに表示します。 • getlist サーバ UTN サーバに接続された USB デバイスの概要 (ポート番号、ベンダ ID、製品 ID、ベンダ名、製品名、デバイスクラス、ステータスなど) を表示します。 • state サーバポート番号 USB ポートに接続された USB デバイスの状態を表示します。
-h または --help	ヘルプページを表示します。

コマンド	説明
-k USB ポートキー または --key USB ポートキー	USB ポートキーを指定します。⇨ 🗎51  **重要：** このコマンドは、USB デバイスを利用できる目的のみで、キーを入力します。 USB キーが毎回自動的に送信されるように、それを正式にシステムに保存するには、-c "コマンド文字列" または --command "コマンド文字列" コマンドを使用します (上記を参照)。 USB ポートキーは、myUTNControl Center ⇨ 🗎51 で設定します。
-mr または --machine readable	getlist コマンド文字列の出力をタブで区切り、find の出力をコンマで区切ります。
-nw または --no-warnings	警告メッセージを抑制します。
-o または --output	コマンドラインの出力を表示します。
-p ポート番号 または --port ポート番号	代替の UTN ポートを使用します。 UTN ポート番号を変更した場合に、このコマンドを使用します (⇨ 🗎29)。
-q または --quiet	出力を抑制します。
-sp ポート番号 または --ssl-port ポート番号	代替の SSL/TLS 暗号化された UTN ポートを で使用します。 UTN SSL ポート番号を変更した場合に、このコマンドを使用します (⇨ 🗎29)。
-t 秒 または timeout 秒	コマンド文字列 activate および deactivate のタイムアウトを設定します。
-v または --version	utnm のバージョン情報を表示します。

リターン情報

コマンドの実行後、リターン情報はコマンドが正常に実行されたかどうかを示します。リターン情報は、戻り値 (リターンコード) と組み合わされたステータスとなります。出力が抑制されると (「--quiet」⇨ 🗎44)、値のみが返されます。

リターン情報は、例えばスクリプトの中で処理を進める方法を決定するために使用することができます。

戻り値	説明
0	コマンドは正常に実行されました。
20	アクティブ化が失敗しました。
21	非アクティブ化が失敗しました。
23	すでにアクティブになっています。
24	すでに非アクティブになっている、または利用できません。
25	アクティブ化が失敗しました。別のユーザがデバイスを含む USB ポートをアクティブにしています。
26	検出されません。USB ポートに接続されたデバイスがない、または USB ポートキー (⇨ 🗎51) が見つからない、もしくは間違っています。
29	検出されません。この VID および PID を持つ USB デバイスが接続されていません。
30	アイソクロナス USB デバイスに対応していません。
31	UTN ドライブエラー。SEH Computertechnik GmbH のサポート部門にご連絡ください。⇨ 🗎4
40	UTN サーバへのネットワーク接続がありません。
41	UTN サーバへの暗号化接続が確立できません。
42	UTN Service への接続がありません。
43	DNS 解決に失敗しました。
44	権限が不十分です (管理者権限が必要です)。
47	この機能には対応していません。
200	エラー (エラーコード表示)

コンソールから utnm を使用する

✓ SEH UTN Manager がクライアントにインストールされていること。⇨ 🗎8
✓ UTN の IP　アドレスまたはホスト名が分かっていること。

1. **コンソール**を開きます。
2. コマンドを入力します。「構文」⇨ 🗎42 および「コマンド」⇨ 🗎42 を参照してください。
3. 入力内容を確認します。

↳ コマンドシーケンスが実行されます。

例：IP アドレス 10.168.1.167 の UTN サーバのポート 3 上にある USB デバイスをアクティブにする

```
utnm -c "activate 10.168.1.167 3"
```

utnm スクリプトを作成する

✓ SEH UTN Manager がクライアントにインストールされていること。⇨ 🗎8
✓ UTN の IP　アドレスまたはホスト名が分かっていること。
✓ 使用するオペレーティングシステム上でスクリプトを作成し使用する方法を理解していること。必要に応じて、オペレーティングシステムの説明書を参照してください。

1. テキストエディタを開きます。
2. コマンドのシーケンスを入力します。「構文」⇨ 🗎42、「コマンド」⇨ 🗎42 および「リターン情報」⇨ 🗎44 を参照してください。
3. ファイルを実行スクリプトとしてクライアントに保存します。

↳ スクリプトが保存されて使用できます。

6 セキュリティ

UTN サーバは、様々なセキュリティメカニズムにより保護することができます。メカニズムが搭載された UTN サーバのみでなく、接続された USB デバイスも保護します。UTN もまた、ネットワークに実装された保護メカニズムの中に組み込むことができます。

- USB 接続を暗号化する方法 ⇨ 🗎46
- myUTN Control Center への接続を暗号化する方法 ⇨ 🗎47
- SSL/TLS 接続の暗号化強度を設定する方法 ⇨ 🗎48
- myUTN Control Center へのアクセスを保護する方法 (ユーザアカウント) ⇨ 🗎49
- UTN サーバのポートをブロックする方法 (TCP ポートアクセス制御) ⇨ 🗎50
- USB デバイスへのアクセスを制御する方法 (myUTN-80 以降のみ) ⇨ 🗎51
- USB デバイスの種類をブロックする方法 ⇨ 🗎52
- 証明書の使用方法 ⇨ 🗎52
- ネットワーク認証を設定する方法 (IEEE 802.1X)」⇨ 🗎57

重要：
myUTN Control Center へのアクセスをユーザアカウントで規制し、セキュリティ関連の設定が不正な改ざんから保護してください。

セキュリティには、SNMP および VLAN も使用できます。
- 「SNMP の設定方法」⇨ 🗎21
- 「VLAN 環境での UTN サーバの利用方法 (myUTN-80 以降のみ)」⇨ 🗎25

6.1 USB 接続を暗号化する方法

USB 接続を保護するには、クライアントと UTN サーバに接続された USB デバイス間のデータ転送を暗号化します。暗号化は、各接続すなわち各 USB ポートを個別にアクティブにする必要があります。

重要：
ペイロードのみが暗号化されます。管理データおよびログデータは、暗号化せずに送信されます。

暗号化プロトコルの SSL (Secure Sockets Layer) とその後継の TLS (Transport Layer Security) が暗号化に使用されます。暗号強度は、暗号化プロトコルと暗号化レベルで設定されます。⇨ 🗎48

警告
SEH UTN Manager は、**低**暗号化レベルに対応していません。暗号化した USB 接続との組合せで**低レベル**をセットアップすると、接続を確立することができません。
できる限り高い暗号化レベルを使用してください。

接続が暗号化されていると、クライアントと UTN サーバは UTN SSL ポートを介して通信します。そのポート番号は、初期値で 9443 です。そのポートがすでに別のアプリケーションなどによりネットワーク内で使用されている場合は、ポート番号を変更することができます。⇨ 🗎29

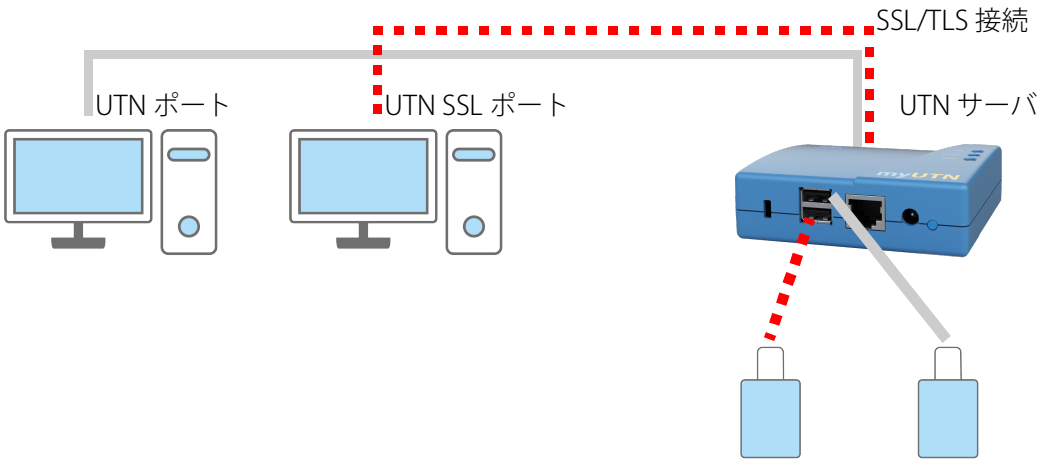


図 6： UTN サーバ - ネットワーク内の SSL/TLS 接続

1. myUTN Control Center を起動します。
2. **セキュリティ – 暗号化**を選択します。
3. USB ポートの暗号化を有効にします。
4. 確定するには、**保存**をクリックします。

↳ クライアントと USB デバイス間のデータ転送が暗号化されます。

暗号化接続は、クライアント側で、SEH UTN Manager のプロパティの下に表示されます。

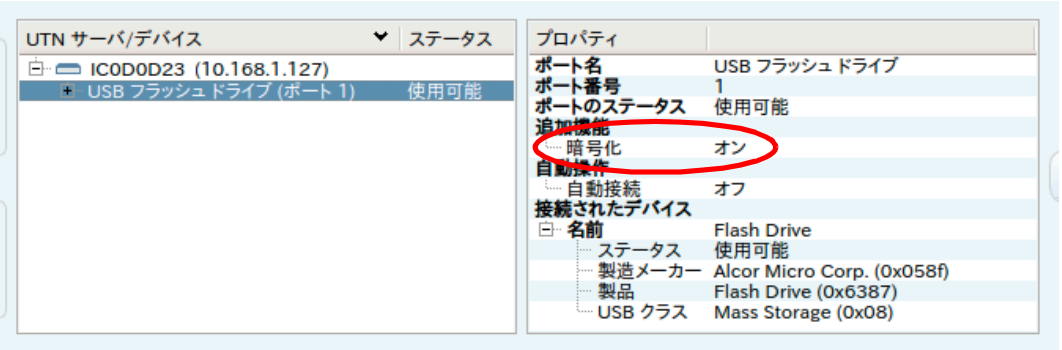


図 7：SEH UTN Manager - 暗号化

6.2 myUTN Control Center への接続を暗号化する方法

myUTN Control Center への 接続は、SSL (Secure Sockets Layer) およびその後継の TLS (Transport Layer Security) プロトコルを使用して暗号化することができます。

- HTTP：非暗号化接続
- HTTPS 暗号化接続
  暗号強度は、暗号化プロトコルと暗号化レベルで設定されます ⇨ 🗎48。暗号化接続の確立が必要になると、クライアントはブラウザを介して証明書を要求します (⇨ 🗎52)。証明書はブラウザが承認できる必要があります。ブラウザソフトウェアの説明書を参照してください。

警告

現在のブラウザは低レベルのセキュリティ設定に対応していません。低レベル設定では接続を確立できません。

次の組合せは使用しないでください：暗号化プロトコル HTTPS と低暗号化レベル

1. myUTN Control Center を起動します。
2. **セキュリティ - デバイスへのアクセス**を選択します。
3. **接続**領域の **HTTP/HTTPS** または **HTTPS のみ**にチェックマークを付けます。
4. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

6.3 SSL/TLS 接続の暗号化強度を設定する方法

UTN サーバに対する接続は双方向とも、SSL (Secure Sockets Layer) およびその後継の TLS (Transport Layer Security) プロトコルを使用して暗号化することができます。

- 電子メール：POP3 (⇨ 🗎23)
- 電子メール：SMTP (⇨ 🗎23)
- myUTN Control Center への Web アクセス：http (⇨ 🗎47)
- クライアントと UTN サーバ (および接続された USB デバイス) 間のデータ転送：USB 接続 (⇨ 🗎48)

暗号化の強度、さらに接続の安全性は暗号化プロトコルと暗号化レベルで設定します。両方とも選択可能です。

各暗号化レベルとは、暗号スイートの集合です。暗号スイートとは、セキュアな接続を確立するために使用される 4 つの暗号アルゴリズムの標準シーケンスで、暗号化強度に基づき暗号化レベルへとグループ化されます。UTN サーバが対応する暗号化レベルを形成する暗号スイートは、選択した暗号化プロトコルにより決定されます。2 つの暗号化レベルから選択できます。

- 任意：暗号化は、通信当事者の双方で自動的にネゴシエートされます。双方が対応する最も高い暗号化が常に選択されます。
- 低レベル：低レベルの暗号化強度の暗号スイートのみを使用します。(高速データ転送)
- 中レベル
- 高レベル：高レベルの暗号化強度の暗号スイートのみを使用します。(低速データ転送)

セキュアな接続を確立する際に、使用するプロトコルと対応する暗号スイートのリストを通信相手に送信します。使用する暗号スイートを取り決めます。初期値では、当事者双方が対応する暗号スイート中で最も強力なスイートが使用されます。

警告

UTN サーバの通信相手が、選択したプロトコルに対応していない場合や、当事者の双方が対応する暗号スイートがない場合、SSL/TLS 接続は確立されません。

問題が発生する場合は、別の設定を選択する、または UTN サーバのパラメータをリセットしてください。⇨ 🗎62

UTN サーバとその通信相手とで自動的に設定をネゴシエートする場合は、双方とも 任意に設定してください。この設定を使用すると、セキュアな接続が確立できる可能性が最も高くなります。

1. myUTN Control Center を起動します。

2. **セキュリティ - SSL 接続**を選択します。
3. **暗号化プロトコル**領域から、任意の暗号化プロトコルを選択します。

警告
現在のブラウザは **SSL** に対応していません。使用するブラウザが最新のバージョンで、myUTN Control Center へのアクセスに **SSL** および **HTTPS のみ**の組合せを設定している場合 (⇨ 🗎47) は、接続が確立できません。
TLS (および SSL 以外) を使用してください。

重要：
UTN サーバが対応するプロトコルは、製品のハードウェアおよびインストールされたファームウェア / ソフトウェアにより異なります。

4. **暗号化レベル**領域から、任意の暗号化レベルを選択します。

警告
現在のブラウザは、**低**レベルの暗号スイートに対応していません。使用するブラウザが最新のバージョンで、myUTN Control Center へのアクセスに**低レベル** および **HTTPS のみ**の組合せを設定している場合 (⇨ 🗎47) は、接続が確立できません。
できる限り高い暗号化レベルを使用してください。

警告
SEH UTN Manager は、**低**暗号化レベルに対応していません。暗号化した USB 接続 (⇨ 🗎46) との組合せで**低レベル**をセットアップすると、接続を確立することができません。
できる限り高い暗号化レベルを使用してください。

5. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

個別の SSL/TLS 接続状態の詳細 (対応する暗号スイートなど) は、SSL 接続の状態 - 詳細の詳細ページを参照してください。

6.4 myUTN Control Center へのアクセスを保護する方法 (ユーザアカウント)

初期値では、UTN をネットワーク内で検出できる場合、myUTN Control Center にアクセスできるユーザに制限はありません。UTN を不正な設定から保護するために、2 種類のユーザアカウントをセットアップできます。

- 管理者：myUTN Control Center へのフルアクセス。対象のユーザは、すべてのページの設定を変更することができます。
- 読み取り専用ユーザ：myUTN Control Center への最小限のアクセス。対象のユーザは、「ホーム」ページのみを閲覧できます。

ユーザアカウントをセットアップした後で myUTN Control Center を起動するとログイン画面が表示されます。2 種類のログイン画面から選択できます。

- ユーザのリスト：ユーザ名が表示されます。パスワードの入力のみが必要です。
- 名前とパスワードのダイアログ：ニュートラルなログイン画面で、ユーザ名とパスワードの入力が必要です。(より高い保護度)

ユーザアカウントによりマルチログインが可能になります。アカウントはユーザ単独でもユーザのグループでも使用できます。同時に最大 16 ユーザまでログインできます。

重要：
myUTN Control Center アクセスのユーザアカウントは SNMP にも使用します ⇨ 🗎21。ユーザアカウントのセットアップ時に考慮してください。

より強力なセキュリティとして、セッションタイムアウトを使用することができます。設定したタイムアウト時間内にまったく操作をしなかった場合、ユーザは自動的にログアウトされます。

1. myUTN Control Center を起動します。
2. **セキュリティ - デバイスへのアクセス**を選択します。
3. 2 種類のユーザアカウントを設定します。**ユーザアカウント**の領域で、**ユーザ名**と**パスワード**を入力します。

パスワードの入力内容を確認する場合は、文字として表示することができます。

4. **Control Center へのアクセス制限**にチェックマークを付けます。
5. ログイン画面の種類を、**ユーザのリスト**と**名前とパスワード**から選択します。
6. **セッションタイムアウト**にチェックマークを付け、**セッション時間**欄にタイムアウトが有効になる時間を分単位で入力します。
7. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

6.5 UTN サーバのポートをブロックする方法 (TCP ポートアクセス制御)

UTN サーバへのアクセスを、「TCP ポートアクセス制御」を使用してポートをブロックすることで制限できます。ポートをブロックすると、このポートを使用するプロトコルやサービスは UTN サーバとの接続を確立できなくなるため、攻撃による影響が少なくなります。

セキュリティレベルでブロックするポートの種類を設定します：

- UTN アクセス (UTN ポートのブロック)
- TCP アクセス (TCP ポート：HTTP/HTTPS/UTN のブロック)
- すべてのポート (IP ポートのブロック)

例外を設定して、クライアントや DNS サーバなどの任意のネットワーク構成要素が UTN サーバとの接続を確立できるようにする必要があります。

警告
「テストモード」では、設定をテストするときにユーザ自身は除外されないように、初期値でアクティブに設定されています。UTN が再起動するまで設定はアクティブになり、以降のアクセスは制限されません。

設定のテストが正常に終了後、アクセス制御が正式に設定されるように、テストモードを非アクティブにする必要があります。

1. myUTN Control Center を起動します。
2. **セキュリティ - TCP ポートアクセス**を選択します。
3. **ポートアクセス制御**にチェックマークを付けます。
4. **セキュリティレベル**領域から、任意の暗号化レベルを選択します。
5. **例外**領域で、UTN サーバにアクセスするネットワーク構成要素を設定します。IP または MAC (ハードウェア) アドレスを入力して、オプションにチェックマークを付けます。

重要：

- MAC アドレスはルータを通して配信されません。
- ワイルドカード (*) を使用すると、サブネットワークを指定できます。

6. **テストモード**が有効であることを確認します。
7. **保存して再起動する**をクリックして確定します。
   設定が保存されます。
   デバイスを再起動するまで、ポートアクセス制御はアクティブです。
8. myUTN Control Center に接続できることを確認する場合は、ポートアクセスをチェックします。

重要：

myUTN Control Center に接続できない場合は UTN サーバを再起動してください ⇨ 🗎60。

9. **テストモード**を非アクティブにします。
10. **保存して再起動する**をクリックして確定します。

↳ 設定が保存されます。

6.6 USB デバイスへのアクセスを制御する方法 (myUTN-80 以降のみ)

USB ポートと接続された USB デバイスへの接続を制限できます。

- USB ポートキー制御：USB ポートにキーが設定されています。USB ポートと接続された USB デバイスのいずれも SEH UTN Manager に表示されず、USB デバイスは使用できません。USB ポートのキーが SEH UTN Manager に入力されている場合のみ、USB ポートおよび接続された USB デバイスが表示されます。
- USB ポートのデバイスの割り当て：特定の USB デバイスが USB ポートに接続されます。これは USB ポートと USB デバイスを、USB デバイスのベンダ ID (VID) および製品 ID (PID) とリンクさせることで実現します。VID と PID の組合せは特定の USB デバイス機種に固有です。この特定機種の USB デバイスのみが USB ポートで使用できます。この方法により、USB デバイスを他のポートに接続してもセキュリティ設定を迂回できないことが保証されます。

セキュリティの要件から、使用していないポートの電源をオフにしてください ⇨ 🗎28。

- USB ポートキーをセットアップする ⇨ 🗎51
- USB ポートキーを入力する (USB デバイスを解除する) ⇨ 🗎52
- USB ポートのデバイス割り当てをセットアップする ⇨ 🗎52

USB ポートキーをセットアップする

USB ポートのキーが myUTN Control Center に設定されています。

1. myUTN Control Center を起動します。
2. **セキュリティ - USB ポートアクセス**を選択します。
3. 任意の USB ポートの**方法**リストに進み**ポートのキー制御**を選択します。
4. **キーの生成**をクリックする、または**キー**欄に任意のキーを (最大 64 ASCII 文字で) 入力します。
5. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。USB デバイスへのアクセスが保護されます。

機能を非アクティブにするには、方法リストに進み --- を選択します。

USB ポートキーを入力する (USB デバイスを解除する)

USB ポートのキー制御で保護された USB デバイスを利用するには、対応するキーをクライアントの SEH UTN Manager に入力する必要があります。

1. SEH UTN Manager を起動します。
2. 選択リストから UTN サーバを選択します。
3. メニューバーから、**UTN サーバ – USB ポートキーの設定**を選択します。
   USB ポートキーの設定ダイアログが表示されます。
4. 対応する USB ポートのキーを入力します。
5. **OK** をクリックします。

↳ アクセスが許可されます。USB ポートと接続された USB デバイスが選択リストに表示され、使用できるようになります。

USB ポートのデバイス割り当てをセットアップする

1. myUTN Control Center を起動します。
2. **セキュリティ - USB ポートアクセス**を選択します。
3. 任意の USB ポートの**方法**リストに進み**デバイス割り当て**を選択します。
4. **デバイスの再割り当て**をクリックします。
   USB デバイス欄に、USB デバイスの VID および PID が表示されます。
5. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。割り当てられた USB デバイス機種のみが、その USB ポートで操作できるようになります。

機能を非アクティブにするには、方法リストに進み --- を選択します。

6.7 USB デバイスの種類をブロックする方法

USB デバイスは、機能に応じて分類されています。例えば、キーボードのような入力デバイスは「Human Interface Device」(HID) グループに分類されます。

USB デバイスは、HID クラスの USB デバイスとして提供されますが、不正な使用が後を絶ちません (いわゆる「BadUSB」)。

UTN サーバを保護するために、HID クラスに分類される入力デバイスをブロックできます。

1. myUTN Control Center を起動します。
2. **セキュリティ - デバイスへのアクセス**を選択します。
3. **USB デバイス**領域で、**入力デバイス (HID クラス) を無効にする**にチェックマークを付ける、またはチェックマークを外します。
4. 確定するには、**保存**をクリックします。

↳ 設定が保存されます。

6.8 証明書の使用方法

UTN サーバには独自の証明書管理機能があります。ディジタル証明書はデータセットで、人間やオブジェクトまたは組織の識別情報を確認します。TCP/IP ネットワークでは、データの暗号化および通信相手の認証に使用されます。

UTN では次の場合、証明書が必要です。

- 認証メカニズムの EAP-TLS、EAP-TTLS および PEAP に参加する ⇨ 57
- 電子メール通信 (SSL/TLS を介した POP3/SMTP) を保護する ⇨ 23
- クライアントと接続された USB デバイス間の接続を保護する ⇨ 46

- myUTN Control Center (HTTPS) への接続を保護する ⇨ 🗎47

UTN サーバでは次の証明書が使用できます。

- 自己署名証明書 x 1
  UTN サーバにより生成され UTN サーバ自体の署名による証明書です。この証明書は UTN サーバの識別情報を確認します。
- クライアント証明書 (要求した証明書または PKCS#12 証明書) x 1
  この証明書は、認証局 (CA) という付加的な信頼できる機関の協力で UTN サーバの識別情報を確認します。
  - 要求した証明書：最初のステップとして、証明書の要求は UTN サーバ上で生成され認証局に送信されます。次のステップで、認証局は要求に基づき UTN サーバ に対して証明書を作成して署名します。
  - PKCS#12 証明書：証明書の交換フォーマット。UTN サーバ用にパスワード保護された PKCS#12 フォーマットで保存された証明書を、認証局に生成させます。その PKCS#12 ファイル (したがって、その中の証明書) を UTN サーバにトランスポートしてインストールします。
- S/MIME 証明書 x 1
  UTN サーバは、自身が送信する電子メールの署名、暗号化に S/MIME 証明書を使用します。対応する秘密キー (PKCS#12 フォーマット) は、電子メールを検証し必要に応じて復号化できるように、自らの証明書として電子メールプログラム (Mozilla Thunderbird など .) にインストールしておく必要があります。
  (myUTN-80 以降のみ)
- CA 証明書 (ルート CA 証明書) x 1 ～ 32
  認証局に対して識別情報を確認するために発行される証明書です。CA 証明書は、各認証局が発行した証明書を検証するために使用されます。UTN サーバの場合、それは通信相手の証明書で識別情報 (信頼チェーン) を検証するために発行されます。複数のレベルの公開キーインフラストラクチャ (PKIs) に対応しています。

重要：
出荷時には、デフォルト証明書が UTN サーバに保存されています。この証明書は、SEH Computertechnik GmbH が各デバイスごとに発行します。

- 証明書を表示する ⇨ 🗎53
- 自己署名証明書を作成する ⇨ 🗎54
- 証明書を要求しインストールする (要求した証明書) ⇨ 🗎55
- PKCS#12 証明書をインストールする ⇨ 🗎55
- S/MIME 証明書をインストールする (myUTN-80 以降のみ) ⇨ 🗎56
- CA 証明書をインストールする ⇨ 🗎56
- 証明書を削除する ⇨ 🗎56

証明書を表示する

✓ 証明書が UTN サーバにインストールされていること。

1. myUTN Control Center を起動します。
2. **セキュリティ** - **証明書**を選択します。
3. 🔍 アイコンで証明書を選択します。

↳ 証明書が表示されます。

自己署名証明書を作成する

重要：
自動署名証明書の場合、UTN サーバにインストールできるのは 1 つのみです。
新たな証明書を作成する場合は、最初に既存の証明書を削除する必要があります。⇨ 56

1. myUTN Control Center を起動します。
2. **セキュリティ - 証明書**を選択します。
3. **自己署名証明書**をクリックします。
4. 適切なパラメータを入力します。⇨ 表 15 54
5. **作成 / インストール**をクリックします。

↳ 証明書が作成されインストールされます。完了までに数分必要な場合があります。

表15： 証明書作成用パラメータ

パラメータ	説明
Common name (共通名)	任意の証明書名です。(最大 64 半角文字) デバイスと証明書を明確に一致させることができるように、UTN サーバの IP アドレス、またはホスト名を使用してください。
Email address (電子メールアドレス)	UTN サーバの担当者の電子メールアドレスです。 (最大 40 半角文字、任意)
Organization name (組織名)	UTN サーバを使用する会社の名前です。 (最大 64 半角文字)
Organizational unit (組織単位)	会社の部門または課の名前です。 (最大 64 半角文字、任意)
Location (場所)	会社の場所です。 (最大 64 半角文字)
State name (都道府県名)	会社が本拠を置く地域です。 (最大 64 半角文字)
Domain component (ドメインコンポーテント)	付加属性の入力ができます。 (任意入力)
SAN (multi-domain)	Subject Alternative Names (サブジェクトの別名：SAN) の入力ができます。別のホスト名 (ドメインなど) の入力に使用します。 (任意入力。半角 255 文字以内)
Country (国)	会社が本拠を置く国です。ISO 3166 に従い 2 文字の国コードを入力します。 例：DE = ドイツ、GB = 英国、US = 米国
Issued on (発行日)	証明書が有効となる日付を指定します。指定日以降に有効になります。
Expires on (期限切れ日時)	証明書が無効となる日付を指定します。指定日に無効になります。
RSA key length (RSA キー長)	使用する RSA キーの長さを指定します。 - 512 ビット（高速暗号化および復号化） - 768 ビット - 1024 ビット（標準暗号化および復号化） - 2048 ビット（低速暗号化および復号化）

証明書を要求しインストールする (要求した証明書)

認証局により UTN サーバに対して発行された証明書は、UTN サーバで使用できます。

使用するには、最初に証明書要求を作成し、認証局に送信します。認証局は要求に基づき、UTN サーバに対して個別に証明書を作成します。この証明書を UTN サーバにインストールします。

重要：

インストールできる要求した証明書は、UTN サーバで作成された証明書要求に基づき発行された証明書のみです。

ファイルが一致しない場合は、現在の証明書要求に基づき、新たな証明書を要求する必要があります。やり直すには、現在の証明書要求を削除する必要があります。⇨ 56

1. myUTN Control Center を起動します。
2. **セキュリティ** - **証明書**を選択します。
3. **認証要求**をクリックします。
4. 必要なパラメータを入力します。⇨ 表 15 54
5. **要求の作成**をクリックします。
   証明書の要求が送信されます。完了までに数分必要な場合があります。
6. **アップロード**を選択して、要求をテキストファイルに保存します。
7. **OK** をクリックします。
8. テキストファイルを、証明書の要求として認証局に送信します。
   認証局は、証明書を作成して要求元に送信します。

重要：

証明書は「base64」形式であることが必要です。

9. **要求された認証情報**をクリックします。
10. **パスワード**ボックスにパスワードを入力します。
11. **インストール**をクリックします。

↳ 要求した証明書が UTN サーバに保存されます。

PKCS#12 証明書をインストールする

重要：

すでに PKCS#12 証明書が UTN にインストールされている場合は、最初にその証明書を削除してください。⇨ 56

✓ 証明書は「base64」形式であること。

1. myUTN Control Center を起動します。
2. **セキュリティ** - **証明書**を選択します。
3. **PKCS#12 認証情報**をクリックします。
4. PKCS#12 証明書を**認証情報ファイル**欄に入力します。
5. パスワードを入力します。
6. **インストール**をクリックします。

↳ PKCS#12 証明書が UTN サーバにインストールされます。

S/MIME 証明書をインストールする (myUTN-80 以降のみ)

重要：
すでに S/MIME 証明書が UTN にインストールされている場合は、最初にその証明書を削除してください。⇨ 56

✓ 証明書は「pem」形式であること。

1. myUTN Control Center を起動します。
2. **セキュリティ** - **証明書**を選択します。
3. **S/MIME 証明書**をクリックします。
4. S/MIME 証明書を**認証情報ファイル**欄に入力します。
5. **インストール**をクリックします。

↳ S/MIME 証明書が UTN サーバに保存されます。

CA 証明書をインストールする

✓ 証明書は「base64」形式であること。

1. myUTN Control Center を起動します。
2. **セキュリティ** - **証明書**を選択します。
3. **CA 認証情報**をクリックします。
4. CA 証明書を**認証情報ファイル**欄に入力します。
5. **インストール**をクリックします。

↳ CA 証明書が UTN サーバに保存されます。

証明書を削除する

警告
myUTN Control Center への暗号化された (HTTPS ⇨ 47) 接続を確立するには、証明書 (自己署名 /CA/PKCS#12) が必要です。該当する証明書が削除されると、myUTN Control Center に接続できなくなります。
この場合は、UTN サーバを再起動してください ⇨ 60。UTN サーバは、新たな自己署名証明書を生成します。それを使用してセキュアな接続を確立することができます。

✓ 証明書が UTN サーバにインストールされていること。

1. myUTN Control Center を起動します。
2. **セキュリティ** - **証明書**を選択します。
3. アイコンで削除する証明書を選択します。
   証明書が表示されます。
4. **削除**をクリックします。

↳ 証明書が削除されます。

6.9 ネットワーク認証を設定する方法 (IEEE 802.1X)」

認証とは、識別情報の立証および検証です。認証により、許可されたデバイスのみがネットワークにアクセスできるため、不正利用から保護されます。

UTN は、EAP (拡張認証プロトコル) に基づく IEEE 802.1X 規格に従った認証に対応しています。

IEEE 802.1X に従いネットワーク内で認証を使用している場合は、UTN サーバを参加させることができます。

- EAP-MD5 を設定する ⇨ 57
- EAP-TLS を設定する ⇨ 57
- EAP-TTLS を設定する ⇨ 58
- PEAP を設定する ⇨ 58
- EAP-FAST を設定する ⇨ 59

EAP-MD5 を設定する

EAP-MD5 (Message Digest #5) は、RADIUS サーバによるユーザベースの認証方式です。最初に、RADIUS サーバ上で UTN サーバのユーザ (ユーザ名およびパスワード) を作成する必要があります。その後 UTN サーバ上で EAP-MD5 をセットアップします。

✓ UTN サーバのユーザアカウントが RADIUS サーバ上にセットアップされていること。

1. myUTN Control Center を起動します。
2. **セキュリティ** - **認証**を選択します。
3. **認証方法**リストから **MD5** を選択します。
4. RADIUS サーバ上で UTN サーバ用にセットアップするユーザアカウントのユーザ名とパスワードを入力します。
5. **保存して再起動する**をクリックして確定します。

↳ 設定が保存されます。

EAP-TLS を設定する

EAP-TLS (Transport Layer Security) RADIUS サーバによる相互の証明書ベースの認証です。この方法では、UTN サーバと RADIUS サーバが暗号化された TLS 接続を通じて証明書を交換します。

RADIUS サーバと UTN サーバの両方に、CA により署名された有効なデジタル証明書が必要です。したがって、PKI (公開キーインフラストラクチャ) が必要になります。

警告

次の順序に従い作業してください。この順序に従って実行しなかった場合、ネットワーク内で UTN サーバに接続できなくなることがあります。

その場合は、UTN サーバのパラメータをリセットしてください ⇨ 62。

1. UTN サーバ上で証明書の要求を作成します ⇨ 55。
2. 証明書の要求および認証サーバを使用して、証明書を作成します。
3. UTN サーバに要求した証明書をインストールします ⇨ 55。
4. 認証サーバ (RADIUS) の証明書を発行した認証局のルート CA 証明書を UTN にインストールします ⇨ 56。
5. myUTN Control Center を起動します。
6. **セキュリティ** - **認証**を選択します。
7. **認証方法**リストから **TLS** を選択します。
8. **EAP ルート証明書**のリストから、ルート CA 証明書を選択します。
9. **保存して再起動する**をクリックして確定します。

↳ 設定が保存されます。

EAP-TTLS を設定する

EAP-TTLS (Tunneled Transport Layer Security) では、機密情報の交換に TLS で保護されたトンネルが使用されます。この方式は、次の 2 つのフェーズで構成されます。

1. 外部認証：暗号化された TLS (Transport Layer Security) トンネルが UTN サーバと RADIUS サーバ間に作成されます。そのために、RADIUS サーバが、CA の署名済みの証明書を使用して UTN に対し自己認証をします。
2. 内部認証：トンネル内では、認証 (CHAP、PAP、MS-CHAP または MS-CHAPv2 による) が発生します。

✓ UTN サーバのユーザアカウントが RADIUS サーバ上にセットアップされていること。
✓ 接続を確立する間のセキュリティ強化 (オプション) のために、認証サーバ (RADIUS) の証明書を発行した認証局のルート CA 証明書が UTN にインストールされていること ⇨ 56。

1. myUTN Control Center を起動します。
2. **セキュリティ** - **認証**を選択します。
3. **認証方法**リストから **TTLS** を選択します。
4. RADIUS サーバ上で UTN サーバ用にセットアップするユーザアカウントのユーザ名とパスワードを入力します。
5. TLS チャンネル内の通信を保護するための設定を選択します。
6. 接続を確立する間のセキュリティを強化します (オプション)。
   EAP ルート証明書のリストから、ルート CA 証明書を選択します。
7. **保存して再起動する**をクリックして確定します。

↳ 設定が保存されます。

PEAP を設定する

PEAP (保護拡張認識プロトコル) により、暗号化 TLS (Transport Layer Security) トンネルが、UTN サーバと RADIUS サーバ間に確立されます。そのために、RADIUS サーバが、CA の署名済みの証明書を使用して UTN に対し自己認証をします。TLS チャンネルは、付加的な EAP 認証方式 (MSCHAPv2 など) によって保護できる別の接続を確立するために使用されます。

この方式は、EAP-TTLS と非常に類似していますが (⇨ 58)、他の方式は UTN サーバを認証するために使用されます。

✓ UTN サーバのユーザアカウントが RADIUS サーバ上にセットアップされていること。
✓ 接続を確立する間のセキュリティ強化 (オプション) のために、認証サーバ (RADIUS) の証明書を発行した認証局のルート CA 証明書が UTN にインストールされていること ⇨ 56。

1. myUTN Control Center を起動します。
2. **セキュリティ** - **認証**を選択します。
3. **認証方法**リストから **PEAP** を選択します。
4. RADIUS サーバ上で UTN サーバ用にセットアップするユーザアカウントのユーザ名とパスワードを入力します。
5. TLS チャンネル内の通信を保護するための設定を選択します。
6. 接続を確立する間のセキュリティを強化します (オプション)。
   EAP ルート証明書のリストから、ルート CA 証明書を選択します。
7. **保存して再起動する**をクリックして確定します。

↳ 設定が保存されます。

EAP-FAST を設定する

EAP-FAST (Flexible Authentication via Secure Tunneling) は、Cisco 社が開発した特定の EAP 方式です。EAP-TTLS (⇨ 🗎58) および PEAP (⇨ 🗎58) と同様に、セキュアなトンネルがデータ伝送を保護しますが、このサーバは証明書による自己認証をしません。代わりに、PACs (Protected Access Credentials) が使用されます。

✓ UTN サーバのユーザアカウントが RADIUS サーバ上にセットアップされていること。

1. UTN Control Center を起動します。
2. **セキュリティ** - **認証**を選択します。
3. **認証方法**リストから **FAST** を選択します。
4. RADIUS サーバ上で UTN サーバ用にセットアップするユーザアカウントのユーザ名とパスワードを入力します。
5. チャンネル内の通信を保護するための設定を選択します。
6. **保存して再起動する**をクリックして確定します。

↳ 設定が保存されます。

7 メンテナンス

UTN サーバは次の方法でメンテナンスできます。

- UTN サーバを再起動する方法 ⇨ 🗎60
- 更新の手順 ⇨ 🗎60
- 設定をバックアップする方法 ⇨ 🗎61
- パラメータを初期値にリセットする方法 ⇨ 🗎62

7.1 UTN サーバを再起動する方法

パラメータの変更後やアップデート後に、UTN サーバは自動的に再起動します。UTN サーバが認識されない場合は、UTN サーバを手動で再起動することもできます。

- myUTN Control Center から UTN サーバを再起動する ⇨ 🗎60UTN サーバが再起動します。リセットボタンで UTN サーバを再起動する ⇨ 🗎60

myUTN Control Center から UTN サーバを再起動する

1. myUTN Control Center を起動します。
2. **メンテナンス** - **再起動**を選択します。
3. **再起動**をクリックします。

UTN サーバが再起動します。**リセットボタンで UTN サーバを再起動する**

1. デバイスの再起動ボタンを短く押します。

↳ UTN サーバが再起動します。

7.2 更新の手順

UTN サーバは、ソフトウェアおよびファームウェアの更新ができます。新しいファームウェア / ソフトウェアには、新たな機能やエラー修正が含まれています。

UTN サーバにインストールされているファームウェア / ソフトウェアのバージョン番号は、myUTN Control Center のホームページで確認できます。

最新のファームウェア / ソフトウェアのファイルは、次の SEH Computertechnik GmbH ウェブサイトで入手できます：

http://www.seh-technology.jp/services/downloads.html

既存のファームウェア / ソフトウェアのみが更新され、設定は保持されます。

重要：
すべてのアップデートファイルには、専用の「readme」ファイルが付属しています。「readme」ファイルを読み、その指示に従ってください。

1. myUTN Control Center を起動します。
2. **メンテナンス** - **更新**を選択します。
3. アップデートファイルを**ファイルの更新**欄に指定します。
4. **インストール**をクリックします。

↳ 更新が実行されます。その後、UTN サーバが再起動します。

7.3 設定をバックアップする方法

UTN サーバのすべての設定値 (パスワード以外) は、「< デフォルト名 >_parameter.txt」ファイルに保存されます。

このパラメータファイルは、バックアップ用コピーとしてローカルクライアントに保存できます。バックアップにより、常に安定した設定状態が復元できます。

バックアップファイルのパラメータ値は、テキストエディタで編集できます。編集後、そのファイルを 1 台以上の UTN サーバにダウンロードできます。ダウンロード後に、デバイスはそのファイルのパラメータ値を採用します。

パラメータの詳細は 「パラメータリスト」⇨ 🗎69 を参照してください。

Dongleserver の myUTN-800 には自動バックアップ機能もあります。パラメータ値および UTN サーバにインストールされた証明書を、自動的に接続された SD カードに保存します。パラメータや証明書が変更されると、バックアップは自動的に更新されます。設定を別の UTN サーバに転送するには、SD カードをその別デバイスに挿入します。コールドブート (電源の遮断と復旧) 後に、設定は自動的に読み込まれます。

警告

盗難や紛失により SD カードが悪用されると、サーバ環境 (証明書、パスワード) が危険な状態になります。

自動バックアップを使用する場合は、UTN サーバを必要なあらゆる対策で保護しなくてはなりません。

パラメータ値を表示する

1. myUTN Control Center を起動します。
2. **メンテナンス** - **パラメータのバックアップ**を選択します。
3. アイコンをクリックします。

↳ 現在のパラメータ値が表示されます。

パラメータファイルを保存する

1. myUTN Control Center を起動します。
2. **メンテナンス** - **パラメータのバックアップ**を選択します。
3. アイコンをクリックします。
4. ブラウザを使用して「< デフォルト名 >_parameters.txt」ファイルをローカルシステムに保存します。

↳ パラメータファイルがバックアップされます。

パラメータファイルを UTN サーバに読み込む

1. myUTN Control Center を起動します。
2. **メンテナンス** - **パラメータのバックアップ**を選択します。
3. **パラメータファイル**欄に「< デフォルト名 >_parameters.txt」ファイルを指定します。
4. **インポート**をクリックします。

↳ UTN サーバはファイルのパラメータ値を採用します。

自動バックアップ (myUTN-800 のみ)

✓ SD カードが UTN サーバに接続されていること。
✓ SD カードのファイルシステムが FAT12、FAT16、または FAT32 であること。
✓ SD カードに 1 MB の利用できる空き容量があること。

(工場出荷時には、上記の要件が保証されています。)

1. myUTN Control Center を起動します。
2. **メンテナンス** - **SD カード**を選択します。
3. **パラメータのバックアップ**にチェックマークを付けます。
4. **保存**をクリックします。

↳ 設定が保存されます。

7.4 パラメータを初期値にリセットする方法

例えば UTN を別のネットワークに設置する場合、UTN を初期値にリセットすることができます。すべての設定が工場出荷時の設定になります。インストール済みの証明書は削除されません。

重要：

UTN サーバの IP アドレスがリセットにより変更されると、myUTN Control Center への接続が遮断される場合があります。

必要に応じて新しい IP アドレスを設定してください ⇨ 16。

設定は、リモートアクセス (myUTN Control Center) または UTN サーバのリセットボタンにより変更できます。

UTN Control Center のパスワードを忘れた場合、UTN サーバをリセットボタンでリセットすることができます。リセットする場合は、パスワードが必要ありません。

警告

myUTN-800：パラメータをリセットする前に、SD カードを UTN サーバから取り出してください。SD カードを取り出さないと、UTN サーバはカードに保存されたパラメータ値を読み込みます (自動バックアップ ⇨ 61)。

- myUTN Control Center でパラメータをリセットする ⇨ 62 パラメータがリセットされます。リセットボタンでパラメータをリセットする ⇨ 63

myUTN Control Center でパラメータをリセットする

1. myUTN Control Center を起動します。
2. **メンテナンス** - **初期設定**を選択します。
3. **初期設定**をクリックします。
   セキュリティクエリが表示されます。
4. セキュリティクエリを確認します。

パラメータがリセットされます。**リセットボタンでパラメータをリセットする**

リセットボタンにより、UTN サーバのパラメータを初期値にリセットすることができます。

1. リセットボタンを 5 秒間押します。
   UTN サーバが再起動します。
   (Dongleserver myUTN-800 は再起動時にビープ音を発します。)

↳ パラメータがリセットされます。

8 補足

この補足には、用語集やトラブルシューティングおよび本説明書のリストが含まれています。

8.1 用語集

複合 USB デバイス

複合 USB デバイスは、ハブと 1 台以上の USB デバイスから構成され、すべて 1 つの筐体に組み込まれています。ドングルは多くの場合、複合 USB デバイスです。

複合 USB デバイスが UTN サーバの USB ポートに接続されていると、組み込まれている USB デバイスはすべて myUTN Control Center および SEH UTN Manager の選択リストに表示されます。ポート接続がアクティブになると、表示された USB デバイスはすべてそのユーザのクライアントに接続されます。複数の USB デバイスの場合、1 つのみのポート接続をアクティブにすることはできません。

デフォルト名

メーカにより割り当てられたデバイス名で変更することができません。同一の UTN サーバを複数使用している場合は、この名前でデバイスを識別できます。

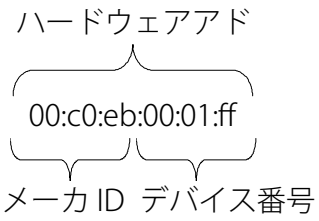
UTN サーバのデフォルト名は、2 つの文字「IC」とデバイス番号で構成されています。デバイス番号は、ハードウェアアドレスの後半の 6 桁で構成されています。

デフォルト名は myUTN Control Center で確認できます。

ハードウェアアドレス

ハードウェアアドレス (イーサネットアドレス、物理アドレスまたは MAC アドレスともいう) は、ネットワークインターフェイスの全世界で通用する一意な識別子です。同一の UTN サーバを複数使用している場合は、この名前でデバイスを識別できます。

メーカが、デバイスのハードウェアにこのアドレスを設定しています。アドレスは 12 個の 16 進数で構成されています。最初の 6 つの数字はメーカを表し、後の 6 つの数字で各デバイスを識別します。数字を区切る文字はプラットフォームにより異なります。Linux ではコロン (:) が使用されます。



ハードウェアアドレスは、筐体上や SEH UTN Manager で確認できます。

myUTN Control Center

myUTN Control Center は UTN サーバのユーザインターフェイスです。UTN サーバは、myUTN Control Center から設定および監視することができます。

myUTNControl Center へはインターネットブラウザ (Mozilla Firefox など) からアクセスします。

詳細はこちら：⇨ 🗎6

SEH UTN Manager

「SEH UTN Manager」は、SEH Computertechnik GmbH が開発したソフトウェアツールです。SEH UTN Manager は、UTN サーバに接続された USB デバイスへの接続を確立し管理するために使用されます。

詳細はこちら：⇨ 🗎8

8.2 トラブルシューティング

この章では、いくつかの不具合を中心に、不具合の内容、状態、修復方法を説明しています。

問題

修復

UTN サーバ：BIOS モード

ファームウェアが正常に機能しソフトウェアに問題がある場合、UTN サーバは BIOS モードに切り替わります。例えば、ソフトウェアの更新が適切ではない場合、BIOS モードになることがあります。

LED が BIOS モードを示します。
- Status LED が消灯
- Activity LED が一定間隔に点滅

警告
BIOS モードでは UTN サーバは利用できません。
当社のサポート部門にご連絡ください ⇨ 🗎4。

UTN サーバ：接続が確立できない

ネットワーク内の UTN サーバを検出し、TCP/IP 接続によりアクセスできますが、SEH UTN Manager からの接続が確立できません。

考えられる原因：

- ファイアウォールや他のセキュリティソフトウェアが通信をブロックしている。
  ファイアウォールやセキュリティソフトウェアの例外に、UTN ポートまたは UTN SSL ポートを追加してください。例外に追加する方法については、該当するファイアウォールやセキュリティソフトウェアの説明書を参照してください。
- SEH UTN Manager 内と UTN サーバ上のポート番号が一致しない。ポート番号を変更したときに SNMPv1 が非アクティブであったため、変更が SEH UTN Manager に送信できません ⇨ 🗎29。

myUTN Control Center：接続が確立できない

考えられるエラー原因を取り除いてください。確認：

- ケーブルの接続

- UTN サーバの IP アドレス ⇨ 🗎16
- ブラウザのプロキシ設定 (詳細はブラウザの説明書を参照してください)

考えられるエラー原因を取り除いた後も、まだ接続が確立できない場合は、次の保護メカニズムが原因の可能性があります。

- SSL/TLS (HTTPS) によりアクセスが制限されている ⇨ 🗎47。
- アクセスが SSL/TLS (HTTPS) により制限され、証明書 (自己署名 /CA/PKCS#12) が削除された ⇨ 🗎52。UTN サーバのパラメータを初期値にリセットしてください ⇨ 🗎62。その過程で新しい証明書が作成されます。

警告

デバイスをリセットするとすべての設定が失われ、IP アドレスも変更される場合があります。

必要に応じて新しい IP アドレスを設定してください ⇨ 🗎16。

- TCP ポートアクセス制御が有効になっている ⇨ 🗎50。
- 暗号化レベルの暗号スイートにブラウザが対応していない ⇨ 🗎48。

myUTN Control Center：ユーザ名やパスワードを忘れた

myUTN Control Center へのアクセスが制限されているときにアクセス認証情報を忘れてしまった場合は、UTN サーバを初期値にリセットすることができます。リセットすると、初期値ではアクセス規制されていない myUTN Control Center を利用できるようになります。

警告

デバイスをリセットするとすべての設定が失われ、IP アドレスも変更される場合があります。

必要に応じて新しい IP アドレスを設定してください ⇨ 🗎16。

SEH UTN Manager：USB デバイスとの接続が確立できない

考えられる原因：

- USB デバイスが、すでに別のクライアントに接続されています。
  他のユーザが接続を終了するのを待つ、またはデバイスをリクエストします ⇨ 🗎37。
- USB デバイスのドライバソフトウェアがクライアントにインストールされていません。
  その USB デバイスのドライバソフトウェアをインストールします。インストールする方法は、該当する USB デバイスの説明書を参照してください。

SEH UTN Manager：USB デバイスが表示されない

考えられるエラー原因を取り除いてください：最初に、UTN サーバに USB デバイスが接続されていることを確認してください。

確認後も USB デバイスがまだ表示されない場合は、次の問題が原因である可能性があります。

- 複数の複合 USB デバイス (⇨ 🗎65) が UTN サーバに接続されている。組み込まれた USB デバイスはそれぞれ、UTN サーバの 仮想 USB ポートを使用しますが、仮想 USB ポートの数は制限されています。制限数に達すると、その UTN サーバではそれ以上 USB デバイスを使用できません (⇨ 🗎35)。
- USB ポートが非アクティブになっている ⇨ 🗎28。
- USB ポートキーが、その USB デバイスに対してアクティブになっている ⇨ 🗎51。
  USB ポートのキーが SEH UTN Manager に入力されているときだけ、USB ポートおよび接続された USB デバイスが表示されます。

SEH UTN Manager：USB ポートには 1 つのデバイスのみが接続されているにもかかわらず、複数の USB デバイスが表示される

考えられる原因：

- USB ハブの が、UTN サーバの USB ポートに接続されている。
- 接続された USB デバイスが、複合 USB デバイスである (⇨ 🗎65)。複合 USB デバイスは、ハブと 1 台以上の USB デバイスから構成され、すべて 1 つの筐体に組み込まれています。USB ポートへの接続が確立されると、表示された USB デバイスはすべてそのユーザのクライアントに接続されて使用できるようになります。

SEH UTN Manager：機能が利用できない、または非アクティブになっている

考えられる原因：

- 使用するクライアントユーザアカウントに、必要な管理者権限がない。それにより、SEH UTN Manager でのユーザ権限も制限されます。詳細は、「SEH UTN Manager – 機能の概要」⇨ 🗎93 の章を参照してください。
  SEH UTN Manager を管理者権限で起動します。方法は、オペレーティングシステムの説明書を参照してください。
- 接続した USB デバイスが、特定の機能に対応していない。

8.3 パラメータリスト

UTN サーバはその設定をパラメータに保存します。パラメータは直接、次の目的に使用します。

- 電子メールによる管理 ⇨ 14
- 設定のバックアップ (パラメータの表示、編集、および他のデバイスへの読込み) ⇨ 61

次の表にすべてのパラメータおよびその値を示します。表を参考に前述の操作に使用することができます。

表16：パラメータリスト - IPv4

パラメータ	値	初期値	説明
ip_addr [IP アドレス]	有効な IP アドレス	169.254.0.0/16	UTN サーバの IP アドレスです。
ip_mask [サブネットマスク]	有効な IP アドレス	255.255.0.0	UTN サーバのサブネットマスクです。 サブネットマスクは、大規模なネットワークをサブネットワークへと論理的に分割するために使用します。UTN サーバをサブネットワークで使用する場合は、サブネットワークのサブネットマスクが必要です。
ip_gate [ゲートウェイ]	有効な IP アドレス	0.0.0.0	UTN サーバが使用するネットワークの標準ゲートウェイの IP アドレスです。 ゲートウェイにより、外部ネットワークから IP アドレスを指定できます。
ip_dhcp [DHCP]	on/off	on	DHCP プロトコルを、有効または無効にします。 DHCP がネットワーク内で有効な場合、IP アドレスは自動的に割り当てられます。
ip_bootp [BOOTP]	on/off	on	BOOTP プロトコルを、有効または無効にします。 BOOTP がネットワーク内で有効な場合、IP アドレスは自動的に割り当てられます。
ip_auto [ARP/PING]	on/off	on	ARP/PING プロトコルを、有効または無効にします。 Zeroconf によって割り当てられた IP アドレスを変更するには、ARP および PING コマンドを使用することができます。この実装状況は、システムにより異なります。使用するオペレーティングシステムの説明書をお読みください。

UTN サーバが IP アドレスを受信した後すぐに、DHCP、BOOTP および ARP/PING を非アクティブにすることを推奨します。

表17：パラメータリスト - IPv6

パラメータ	値	初期値	説明
ipv6 [IPv6]	on/off	on	UTN サーバの IPv6 機能を、有効または無効にします。
ipv6_auto [自動設定]	on/off	on	UTN サーバへの IPv6 アドレスの自動割り当てを、有効または無効にします。
ipv6_addr [IPv6 アドレス]	n:n:n:n:n:n:n:n	: :	IPv6 ユニキャストアドレスを指定します。このアドレスは n:n:n:n:n:n:n:n の形式で UTN サーバに手動で割り当てます。 • 各「n」は、アドレスの 8 つの 16 ビット要素の 1 つの 16 進数の値を示します。 • フィールド内の先頭のゼロは省略できます。 • IPv6 アドレスは、連続するフィールドの内容がすべてゼロ (0) である場合、短縮バージョンを使用して入力または表示できます。この場合、2 つのコロン (::) を使用します。
ipv6_gate [ルータ]	n:n:n:n:n:n:n:n	: :	UTN サーバが要求を送信する宛先の静的ルータを、手動で指定します。
ipv6_plen [プレフィックス長]	0 ～ 64 [1 ～ 2 個の半角文字：0 ～ 9]	64	IPv6 アドレスのサブネットプレフィックスの長さを設定します。64 の値があらかじめ設定されています。 アドレス範囲 (ネットワークなど) は、プレフィックスを使用して指定します。指定するには、プレフィックス長 (使用するビット数) を 10 進数で IPv6 アドレスに追加し、その 10 進数の先頭にスラッシュ (/) を付けます。

表18：パラメータリスト - DNS

パラメータ	値	初期値	説明
dns [DNS]	on/off	on	DNS サーバによる名前解決を、有効または無効にします。
dns_domain [ドメイン名]	最大 255 半角文字 [a ～ z、A ～ Z、0 ～ 9]	[空白]	プライマリ DNS サーバの IP アドレスを指定します。
dns_primary [プライマリ DNS サーバ]	有効な IP アドレス	0.0.0.0	セカンダリ DNS サーバの IP アドレスを指定します。 セカンダリ DNS サーバは、プライマリ DNS サーバが利用できない場合に使用されます。
dns_secondary [セカンダリ DNS サーバ]	有効な IP アドレス	0.0.0.0	既存の DNS サーバのドメイン名を指定します。

表19：パラメータリスト - SNMP

パラメータ	値	初期値	説明
snmpv1 [SNMPv1]	on/off	on	SNMPv1 を有効または無効にします。
snmpv1_ronly [読み取り専用]	on/off	off	コミュニティに対する書き込み禁止を、有効または無効にします。
snmpv1_community [コミュニティ]	最大 64 半角文字 [a ～ z、A ～ Z、 0 ～ 9]	public	SNMP コミュニティ名：監視側装置に設定されている名前を入力します。 **重要：** デフォルト名は「public」です。その名前は、読み取り / 書き込みコミュニティに共通で使用されます。セキュリティの要件から、名前をできるだけ早く変更することを推奨します。
snmpv3 [SNMPv3]	on/off	on	SNMPv3 を有効化または無効化します。
any_hash [ハッシュ]	md5 sha	md5	SNMP ユーザグループ 1 のハッシュアルゴリズムを指定します。
any_rights [アクセス権]	--- readonly readwrite	readonly	SNMP ユーザグループ 1 のアクセス権を設定します。 --- = [なし]
any_cipher [暗号化]	--- aes des	---	SNMP ユーザグループ 1 の暗号化の方法を設定します。 --- = [なし]
admin_hash [ハッシュ]	md5 sha	md5	SNMP ユーザグループ 2 のハッシュアルゴリズムを指定します。
admin_rights [アクセス権]	--- readonly readwrite	readwrite	SNMP ユーザグループ 2 のアクセス権を設定します。 --- = [なし]
admin_cipher [暗号化]	--- aes des	---	SNMP ユーザグループ 2 の暗号化の方法を設定します。

重要：
UTN サーバのユーザアカウントは SNMP ユーザアカウントとしても使用されます ⇨ 21。ユーザアカウントのセットアップ時に考慮してください。

表20：パラメータリスト - Bonjour

パラメータ	値	初期値	説明
bonjour [Bonjour]	on/off	on	Bonjour を有効または無効にします。
bonjour_name [Bonjour 名]	最大 64 半角文字 [a ～ z、A ～ Z、0 ～ 9]	[デフォルト名]	myUTN サーバの Bonjour 名を設定します。 myUTN サーバは、この名前を Bonjour サービスのアナウンスに使用します。Bonjour 名が入力しなかった場合は、デフォルト名 (デバイス名 @ICxxxxxx) が使用されます。

表21：パラメータリスト - POP3 (myUTN-80 以降のみ)

パラメータ	値	初期値	説明
pop3 [POP3]	on/off	off	POP3 の機能を有効または無効にします。
pop3_srv [サーバ名]	最大 128 半角文字	[空白]	POP3 サーバを IP アドレスまたはホスト名で指定します。 ホスト名での指定は、DNS サーバが事前設定されている場合にのみ可能です。
pop3_port [サーバポート]	1 ～ 65535 [1 ～ 5 個の半角文字：0 ～ 9]	110	電子メールの受信用に UTN サーバが使用するポートを指定します。 POP3 のポート番号は 110 です。SSL/TLS (パラメータ「POP3 - セキュリティ」⇨ 23) のデフォルトポート番号は 995 です。必要に応じて、POP3 サーバの説明書を参照してください。
pop3_sec [セキュリティ]	0 ～ 2 [1 桁の数字：0 ～ 2]	0	使用する認証方法を設定します。 • APOP：POP3 サーバにログオンするときにパスワードを暗号化します。 • SSL/TLS：POP3 サーバとの通信全体を暗号化します。暗号強度は、暗号化プロトコルと暗号化レベルで設定されます ⇨ 48。 0 = セキュリティなし 1 = APOP 2 = SSL/TLS
pop3_poll [メールのチェック間隔]	1 ～ 10080 [1 ～ 5 個の半角文字：0 ～ 9]	2	POP3 サーバをチェックして電子メールを確認する時間間隔を分単位で指定します。
pop3_limit [メールサイズの上限]	0 ～ 4096 [1 ～ 4 個の半角文字：0 ～ 9]	4096	UTN サーバが許容する電子メールの最大サイズを Kbyte 単位で設定します。 0 = 無制限
pop3_usr [ユーザ名]	最大 128 半角文字	[空白]	POP3 サーバにログインするために UTN サーバが使用するユーザ名を設定します。
pop3_pwd [パスワード]	最大 128 半角文字	[空白]	POP3 サーバにログインするために UTN サーバが使用するユーザパスワードを設定します。

表22：パラメータリスト - SMTP (myUTN-80 以降のみ)

パラメータ	値	初期値	説明
smtp_srv [サーバ名]	最大 128 半角文字	[空白]	SMTP サーバを IP アドレスまたはホスト名で設定します。 ホスト名での指定は、DNS サーバが事前設定されている場合にのみ可能です。
smtp_port [サーバポート]	1 ～ 65535 [1 ～ 5 個の半角文字：0 ～ 9]	25	UTN サーバおよび SMTP サーバが通信に使用するポートを指定します。 SMTP のデフォルトポート番号は 25 です。SSL/TLS (パラメータ 「SMTP – SSL/TLS」⇨ 24) に対して、SMTP は初期値でポート 587 (STARTSSL/STARTTLS) または以前のポート 465 (SMTPS) を使用します。必要に応じて、SMTP サーバの説明書を参照してください。
smtp_ssl [SSL/TLS]	on/off	off	SSL/TLS を有効または無効にします。 SSL/TLS は UTN から SMTP サーバへの通信を暗号化します。暗号強度は、暗号化プロトコルと暗号化レベルで設定されます ⇨ 48。
smtp_sender [送信者名]	最大 128 半角文字	[空白]	UTN サーバが電子メールの送信に使用する電子メールアドレスを設定します。 多くの場合、送信者の名前と電子メールアカウントのユーザ名は同一になります。
smtp_auth [ログイン]	on/off	off	SNMP の認証 (SMTP AUTH) を有効または無効にします。電子メールを送信する場合、UTN は自己認証のために自らのユーザ名とパスワードを SMTP サーバに送信します。ユーザ名 (パラメータ「SMTP - ユーザ名」⇨ 24) およびパスワード (パラメータ「SMTP - パスワード」⇨ 24) を入力します。 SMTP サーバの中には、不正使用 (スパム) を防止するために SMTP 認証を必要とするものがあります。
smtp_usr [ユーザ名]	最大 128 半角文字	[空白]	SMTP サーバにログインするために UTN サーバが使用するユーザ名を設定します。
smtp_pwd [パスワード]	最大 128 半角文字	[空白]	SMTP サーバへのログインに使用する UTN サーバのパスワードを設定します。
smtp_sign [セキュリティ (S/MIME)]	on/off	off	電子メールセキュリティ規格の S/MIME (Secure/Multipurpose Internet Mail Extensions) を、有効または無効にします。S/MIME は、電子メールの署名 (パラメータ「SMTP - 電子メールの署名」⇨ 24) または暗号化 (パラメータ「SMTP - 完全な暗号化」⇨ 24) に使用します。対象の機能を (「SMTP - 公開キーの添付」⇨ 25 により) 有効にします。

パラメータ	値	初期値	説明
smtp_attpkey [公開キーの添付]	on/off	on	公開キーを電子メールと一緒に送信します。多くの電子メールクライアントが、電子メールを表示するキーを必要とします。
smtp_encrypt [完全な暗号化] [電子メールの署名]	on/off	off	on = 電子メールの暗号化をアクティブにします。暗号化された電子メールは、対象の受信者のみが開いて読むことができます。暗号化には S/MIME 証明書が必要です ⇨ 52。 off = 電子メールの署名をアクティブにします。受信者は、署名を使用して送信者の識別情報をチェックできます。署名は電子メールが改ざんされていないことを証明します。 電子メールに署名を使用するには S/MIME 証明書が必要です。⇨ 52

表23：パラメータリスト - IPv4-VLAN (myUTN-80 以降のみ)

パラメータ	値	初期値	説明
ip4vlan_mgmt [IPv4 管理 VLAN]	on/off	off	IPv4 管理 VLAN データの転送を、有効または無効にします。 この設定を有効にした場合、SNMP は IPv4 管理 VLAN でのみ利用できます。
ip4vlan_mgmt_id [VLAN ID]	0 ～ 4096 [1 桁から 4 桁の数字：0 ～ 9]	0	IPv4 管理 VLAN を識別するための ID です。
ip4vlan_mgmt_any [任意の VLAN からのアクセス]	on/off	off	IPv4 クライアント VLAN を介した UTN サーバへの管理者アクセス (Web) を、有効または無効にします。 この設定が有効な場合、UTN サーバはすべての VLAN を介して管理できます。
ip4vlan_mgmt_untag [LAN からのアクセス (タグなし)]	on/off	on	タグなしの IPv4 パケットを介した UTN サーバへの管理者アクセスを、有効または無効にします。この設定が無効な場合、UTN サーバは VLAN を介してのみ管理できます。
ipv4vlan_on_1 ～ ipv4vlan_on_20 [VLAN]	on/off	off	IPv4 クライアント VLAN データの転送を、有効または無効にします。
ipv4vlan_addr_1 ～ ipv4vlan_addr_20 [IP アドレス]	有効な IP アドレス	192.168.0.0	IPv4 クライアント VLAN 内にある UTN サーバの IP アドレスです。
ipv4vlan_mask_1 ～ ipv4vlan_mask_20 [サブネットマスク]	有効な IP アドレス	255.255.255.0	IPv4 クライアント VLAN 内にある UTN サーバのサブネットマスクです。
ip4vlan_gate_1 ～ ip4vlan_gate_20 [ゲートウェイ]	有効な IP アドレス	0.0.0.0	IPv4 管理 VLAN での IP ゲートウェイアドレスゲートウェイにより、外部ネットワークから IP アドレスを指定できます。
ipv4vlan_id_1 ～ ipv4vlan_id_20 [VLAN ID]	0 ～ 4096 [1 ～ 4 個の半角文字：0 ～ 9]	0	IPv4 クライアント VLAN を識別するための ID です。
utn_2vlan_1 ～ utn_2vlan_20 [VLAN の割り当て]	0 ～ 9 [1 桁の数字： 0 ～ 9]	0	USB ポートに VLAN を割り当てます。 0 = すべて 1 = VLAN 1 2 = VLAN 2 など 9 = なし

表24：パラメータリスト - WLAN (myUTN-55 のみ)

パラメータ	値	初期値	説明
wifimode [モード]	adhoc infra	adhoc	通信モード (ネットワークインフラストラクチャ) を指定します。 • アドホック：WLAN は分散化されたアドホックネットワークで、デバイスがお互いに (ピアツーピアで) 通信します。 • インフラストラクチャ：WLAN は、アクセスポイント / ルータが中央の通信ハブとして機能するインフラストラクチャネットワークです。アクセスポイントは、固定ネットワークにケーブル接続されています。
wifiname [ネットワーク名 (SSID)]	最大 64 半角文字 [a ～ z、A ～ Z、0 ～ 9、_、-]	SEH	SSID (Service Set Identifier) としても知られている WLAN のネットワーク名を入力します。
wifichannel [チャンネル]	1 ～ 14 [1 ～ 2 個の半角文字：0 ～ 9]	3	WLAN のチャンネル (周波数範囲) を入力します。 (アドホックモードのみ)  **警告** 国から許可された WLAN チャンネルのみを使用してください。 UTN は、多くのチャンネルに対応するグローバルな製品です。一方で、チャンネルは各国の法令によって規制されています。したがって、UTN は使用する国で禁止されたチャンネルにも対応している場合があります。 国の規制には、各自が注意してください。
wifiencrypt [暗号化方式]	--- WepOpen WepShared TKIP AES TKIP2 AES2 AESTKIP AESTKIP2 Auto	---	WLAN を保護する暗号化方式を選択します。 --- = なし WepOpen = WEP (オープンシステム) WepShared = WEP (共有キー) TKIP = WPA (TKIP) AES = WPA (AES) TKIP2 = WPA2 (TKIP) AES2 = WPA2 (AES) AESTKIP = WPA (AES/TKIP) AESTKIP2 = WPA2 (AES/TKIP) Auto = WPA (自動)

パラメータ	値	初期値	説明
wifikeyid [WEP キーを使用]	0 ～ 4 [1 桁の数字： 0 ～ 4]	0	使用する WEP キーを指定します。 0 = キーなし 1 = キー 1 2 = キー 2 3 = キー 3 4 = キー 4
wifiwkey1 ～ wifiwkey4 [キー 1 ～ 4]	キーの種類により異なります。 文字数： 64 ASCII= 5 64 HEX = 10 128 ASCII= 13 128 HEX= 26 文字セット： 16 進数 = 0 ～ 9、a ～ f、A ～ F ASCII = 0 ～ 9、a ～ z、A ～ Z	[空白]	WEP キーを指定します。4 つの WEP キーが利用できます。 **重要：** WEP には 16 進数キーを使用することを推奨します。 アクセスポイント / ルータによっては、ASCII フォーマットの WEP キーを 16 進数フォーマットへ変換します。この場合は、UTN サーバ上の ASCII キーとアクセスポイント / ルータ上の 16 進数が一致しません。
wifipsk [PSK]	8 ～ 63 個の半角文字	[空白]	WPA (Wi-Fi Protected Access) 用の PSK (Pre Shared Key) を指定します。
wifiroaming [ローミング]	on/off	off	ローミング (アクセスポイント / ルータの切り替え) を、有効または無効にします。複数の (同一設定の) アクセスポイント / ルータがある広域に跨る WLAN で UTN サーバの位置を変更すると、ローミングがアクティブな場合に、UTN サーバは接続ロスのない良好な信号へと自動的に切り替わります。 (インフラストラクチャモードのみ)

表25：パラメータリスト - 日付/時間

パラメータ	値	初期値	説明
ntp [日付 / 時間]	on/off	on	タイムサーバ (SNTP) の使用を、有効または無効にします。
ntp_server [タイムサーバ]	最大 64 半角文字 [a ～ z、A ～ Z、0 ～ 9]	pool.ntp.org	タイムサーバを IP アドレスまたはホスト名で指定します。 ホスト名での指定は、DNS サーバがあらかじめ設定されている場合にのみ可能です。 **重要：** 適切に設定されたネットワーク上で、UTN サーバはタイムサーバ設定を DHCP により自動的に受信します。自動的に割り当てられたタイムサーバは、手動設定より常に優先されます。
ntp_tzone [タイムゾーン]	UTC、GMT、EST、EDT、CST、CDT、MST、MDT、PST、PDT など。	CET/CEST (EU)	協定世界時 (UTC) を、地域および国独自の制度 (夏時間など) に従い補正します。

表26：パラメータリスト - 説明

パラメータ	値	初期値	説明
sys_name [ホスト名]	最大 64 半角文字 [a ～ z、A ～ Z、0 ～ 9]	[空白]	IP アドレスに代わるデバイス名。名前により、例えば複数の UTN サーバを使用している場合、ネットワーク上で UTN サーバを容易に識別できます。 myUTN Control Center および SEH UTN Manager に表示されます。
sys_descr [説明]	最大 64 半角文字 [a ～ z、A ～ Z、0 ～ 9]	[空白]	場所や所属部門などのデバイスの説明。 myUTN Control Center および SEH UTN Manager に表示されます。
sys_contact [担当者]	最大 64 半角文字 [a ～ z、A ～ Z、0 ～ 9]	[空白]	デバイス管理者などの担当者。 myUTN Control Center に表示されます。

表27：パラメータリスト - USB ポート

パラメータ	値	初期値	説明
utn_tag_1 ～ utn_tag_20 [ポート名]	最大 32 半角文字 [a ～ z、A ～ Z、 0 ～ 9]	[空白]	USB ポートの名前を任意で入力します。
utn_poff1 ～ utn_poff20 [ポート]	on/off	off	USB ポート (ポートに接続された USB デバイス) への電源供給を、無効または有効にします。 off= 電源有効 on = 電源無効

表28：パラメータリスト - UTN ポート

パラメータ	値	初期値	説明
utn_port [UTN ポート]	1 ～ 9200 [1 ～ 4 個の半角文字：0 ～ 9]	9200	UTN ポート (暗号化接続用) の数を指定します。 **警告** UTN ポートをファイアウォールでブロックしないでください。
utn_sslport [UTN SSL ポート]	1 ～ 9443 [1 ～ 4 個の半角文字：0 ～ 9]	9443	UTN SSL ポート (暗号化接続用) の数を指定します。 **警告** UTN SSL ポートをセキュリティソフトウェア (ファイアウォール) でブロックしないでください。

表29：パラメータリスト - 通知 (myUTN-80 以降のみ)

パラメータ	値	初期値	説明
mailto_1 mailto_2 [電子メールアドレス]	有効な電子メールアドレス 最大 64 半角文字	[空白]	通知の受信者の電子メールアドレスを設定します。
noti_stat_1 noti_stat_2 [ステータス通知]	on/off	off	受信者 1 または 2 への定期的なステータス通知を、有効または無効にします。
notistat_d [間隔]	al su mo tu we th fr sa	al	ステータス通知を送信する日 (間隔) を指定します。 al= 毎日 su= 日曜日 mo= 月曜日 tu= 火曜日 we= 水曜日 th= 木曜日 fr= 金曜日 sa= 土曜日
notistat_h [時]	0 ～ 23 [1 ～ 2 個の半角文字：0 ～ 9]	0	ステータス通知を送信する時 (時間) を指定します。 1 = 1 時間 2 = 2 時間 3 = 3 時間 など
notistat_tm [分]	0 ～ 5 [1 桁の数字： 0 ～ 5]	0	ステータス通知を送信する時 (分) を指定します。 0 = 00 分 1 = 10 分 2 = 20 分 3 = 30 分 4 = 40 分 5 = 50 分
noti_dev_1 noti_dev_2 [USB デバイスが接続または切断された場合に電子メールを送信]	on/off	off	USB デバイスが UTN サーバに接続された後、または UTN サーバから取り外された後の電子メール通知を、有効または無効にします。
noti_act_1 noti_act_2 [USB ポートがアクティブまたは非アクティブになったときに電子メールを送信]	on/off	off	USB ポート (すなわち接続された USB デバイスへの接続) がアクティブまたは非アクティブになった後の電子メール通知を、有効または無効にします。

パラメータ	値	初期値	説明
noti_pup_1 noti_pup_2 [UTN サーバが再起動した場合に電子メールを送信]	on/off	off	UTN サーバが再起動したときの電子メール通知を、有効または無効にします。
noti_pwr_1 noti_pwr_2 [電源が遮断または接続されたときに電子メールを送信]	on/off	off	UTN サーバの 2 つの電源のうち 1 つが遮断または接続されたときの電子メール通知を、有効または無効にします。 (myUTN-800 のみ)
noti_lnk_1 noti_lnk_2 [ネットワーク接続が遮断または確立されたときに電子メールを送信]	on/off	off	UTN サーバの 2 つのネットワーク接続のうち 1 つが遮断または接続されたときの電子メール通知を、有効または無効にします。 (myUTN-800 のみ)
noti_sdinout_1 noti_sdinout_2 [SD カードが接続または切断されたときに電子メールを送信]	on/off	off	SD カードが UTN サーバに接続された後、または UTN サーバから取り外された後の電子メール通知を、有効または無効にします。 (myUTN-800 のみ)
noti_sdunusable_1 noti_sdunusable_2 [SD カードが使用できないときに電子メールを送信]	on/off	off	SD カードが使用できない場合の電子メール通知を、有効または無効にします。 (myUTN-800 のみ)
trapto_1 trapto_2 [アドレス]	有効な IP アドレス	0.0.0.0	受信者の SNMP トラップアドレスです。
trapcommu_1 trapcommu_2 [コミュニティ]	最大 64 半角文字 [a ～ z、A ～ Z、 0 ～ 9]	public	受信者の SNMP トラップコミュニティです。
trapdev [USB デバイスが接続または切断されたときにトラップを送信]	on/off	off	USB デバイスが UTN サーバに接続された後、または UTN サーバから取り外された後の SNMP トラップ通知を、有効または無効にします。
trapact [USB ポートがアクティブまたは非アクティブになったときにトラップを送信]	on/off	off	USB ポート (接続された USB デバイスへの接続など) がアクティブまたは非アクティブになった後の SNMP トラップ通知を、有効または無効にします。

パラメータ	値	初期値	説明
trappup [UTN サーバが再起動した場合にトラップを送信]	on/off	off	UTN サーバが再起動したときの SNMP トラップの送信を、有効または無効にします。
trap_pwr [電源が切断または接続されたときにトラップを送信]	on/off	off	UTN サーバの 2 つの電源のうち 1 つが遮断または接続されたときの SNMP トラップ通知を、有効または無効にします。 (myUTN-800 のみ)
trap_lnk [ネットワーク接続が遮断または確立されたときにトラップを送信]	on/off	off	UTN サーバの 2 つのネットワーク接続のうち 1 つが遮断または接続されたときの SNMP トラップ通知を、有効または無効にします。 (myUTN-800 のみ)
trap_sdinout [SD カードが接続または切断されたときにトラップを送信]	on/off	off	SD カードが UTN サーバに接続された後、または UTN サーバから取り外された後の SNMP トラップ通知を、有効または無効にします。 (myUTN-800 のみ)
trap_sdunusable [SD カードが使用できないときにトラップを送信]	on/off	off	SD カードが使用できない場合の SNMP トラップ送信を、有効または無効にします。 (myUTN-800 のみ)

表30：パラメータリスト – ディスプレイ (myUTN-800 のみ)

パラメータ	値	初期値	説明
dis_def [識別子 (ディスプレイパネル)]	1 ～ 2 個の半角文字 [A–Z、0–9、E+ 数字の組合せは、エラーに使用するので、指定できません ⇨ 31。]	SD	UTN サーバの前面のディスプレイパネルに表示される名前 (ID) を設定します。
dis_pwr [1 個の電源だけが電力を供給しているときにエラーを表示]	on/off	on	2 つの電源のうち 1 つだけが、UTN サーバに電力を供給しているときにディスプレイパネルに表示するエラーを、有効または無効にします。 エラーはコードで表示されます ⇨ 31。
disp_sdc [SD カードのエラーを表示]	on/off	on	UTN サーバに SD カードが挿入されていない、または SD カードが使用できないときにディスプレイパネルに表示するエラーメッセージを、有効または無効にします。 エラーはコードで表示されます ⇨ 31。
disp_lnk [1 つのネットワーク接続のみが確立されたときにエラーを表示]	on/off	on	UTN サーバの 2 つのネットワーク接続のうち 1 つのみが確立されたときにディスプレイパネルに表示されるエラーメッセージを、有効または無効にします。 エラーはコードで表示されます ⇨ 31。

表31：パラメータリスト - 音響信号 (myUTN-800 のみ)

パラメータ	値	初期値	説明
beepPwr [1 個の電源のみが電力を供給]	on/off	off	UTN サーバに 2 つの電源のうち 1 つのみが電源を供給しているときに発信される音響信号を、有効または無効にします。
beepSDc [SD カードエラー]	on/off	off	UTN サーバに挿入された SD カードがない、または SD カードが使用できないときに発信される音響信号を、有効または無効にします。
beepLnk [1 つのネットワーク接続のみが確立]	on/off	off	UTN サーバの 2 つのネットワーク接続のうち 1 つのみが確立したときに発信される音響信号を、有効または無効にします。

表32：パラメータリスト - SSL/TLS 接続

パラメータ	値	初期値	説明
sslmethod [暗号化プロトコル]	any sslv3 tls10 tls11 tls12	any	SSL/TLS 接続に使用する暗号化プロトコルを指定します。 any = 任意 (自動ネゴシエーション) sslv3 = SSL 3.0 tls10 = TLS 1.0 tls11 = TLS 1.1 tls12 = TLS 1.2 **警告** 現在のブラウザは低レベルのセキュリティ設定に対応していません。現在のブラウザと HTTPS のみの設定で myUTN Control Center (⇨ 🗎47) へのアクセスに SSL を使用すると、接続は確立できません。 TLS (および SSL 以外) を使用してください。
セキュリティ [暗号化レベル]	1 ～ 4 [1 桁の数字： 1 ～ 4]	4	SSL/TLS 接続に使用する暗号化レベルを指定します。 1 = low (低) 2 = medium (中) 3 = high (高) 4 = any (自動ネゴシエーション) **警告** 現在のブラウザは、**低**レベルの暗号スイートに対応していません。現在のブラウザと HTTPS のみの設定で myUTN Control Center (⇨ 🗎47) へのアクセスに低レベルを使用すると、接続は確立できません。 できる限り高い暗号化レベルを使用してください。 **警告** SEH UTN Manager は、**低**暗号化レベルに対応していません。暗号化した USB 接続との組合せで**低レベル**をセットアップすると、接続を確立することができません。 できる限り高い暗号化レベルを使用してください。

表33：パラメータリスト - myUTN Control Center セキュリティ

パラメータ	値	初期値	説明
http_allowed [接続]	on/off	on	myUTN Control Center への接続に使用する接続タイプ (HTTP/HTTPS) を指定します。 on = HTTP/HTTPS off= HTTPS のみ 暗号強度は、暗号化プロトコルと暗号化レベルで設定されます ⇨ 🗎48。 **警告** 現在のブラウザは低レベルのセキュリティ設定に対応していません。低レベル設定では接続を確立できません。 次の組合せは使用しないでください：暗号化プロトコル HTTPS と低暗号化レベル 。 接続が確立すると、UTN サーバの識別情報が検証されます。そのために、クライアントはブラウザから証明書を要求します (⇨ 🗎52)。証明書はブラウザが承認できる必要があります。ブラウザソフトウェアの説明書を参照してください。
sessKeys [Control Center へのアクセス制限]	on/off	off	myUTN Control Center のユーザアカウントを、有効または無効にします。有効の場合は、myUTN Control Center が起動するときにログイン画面が表示されます。 **重要：** ユーザアカウント (ユーザ名およびパスワード) を設定します。
admin_name [管理者 - ユーザ名]	最大 64 半角文字 [a ～ z、A ～ Z、0 ～ 9]	admin	管理者ユーザアカウント用のユーザ名を設定します。 **重要：** SNMPv3 admin アカウントのユーザ名も設定します ⇨ 🗎21。
admin_pwd [管理者 - パスワード]	8 ～ 64 個の半角文字 [a ～ z、A ～ Z、0 ～ 9]	administrator	管理者ユーザアカウント用のパスワードを設定します。 **重要：** SNMPv3 admin アカウントのパスワードも設定します ⇨ 🗎21。
any_name [読み取り専用ユーザ - ユーザ名]	最大 64 半角文字 [a ～ z、A ～ Z、0 ～ 9]	anonymous	読み取り専用ユーザアカウント用のユーザ名を設定します。 **重要：** SNMPv3 ユーザアカウントのユーザ名も設定します ⇨ 🗎21。

パラメータ	値	初期値	説明
any_pwd [読み取り専用ユーザ - パスワード]	最大 64 半角文字 [a ～ z、A ～ Z、0 ～ 9]	[空白]	読み取り専用ユーザアカウント用のパスワードを設定します。 **重要：** SNMPv3 ユーザアカウントのパスワードも設定します ⇨ 21。
sessKeyUList [ログイン画面の表示]	on/off	on	ログイン画面の種類を設定します。 on= ユーザリストを表示します。パスワード入力のみが必要になります。 off= ニュートラルなログイン画面で、ユーザ名とパスワードの入力が必要です。
sessKeyTimer [セッションタイムアウト]	on/off	on	セッションタイムアウトを有効または無効にします。
sessKeyTimeout [セッションタイムアウト]	120 ～ 3600 [3 ～ 4 個の半角文字：0 ～ 9]	600	タイムアウトが有効になるまでの時間 (秒単位)。

表34：パラメータリスト - TCP ポートアクセス

パラメータ	値	初期値	説明
protection [ポートアクセス制御]	on/off	off	選択されたポートの UTN サーバなどへの接続のブロッキングを、有効または無効にします。
protection_level [セキュリティレベル]	protec_utn protec_tcp protec_all	protec_utn	ブロックするポートタイプを指定します。 protec_utn= UTN アクセス (UTN ポート) protec_tcp= TCP アクセス (TCP ポート：HTTP/HTTPS/UTN) protec_all= すべてのポート (IP ポート)
ip_filter_on_1 ～ ip_filter_on_8 [IP アドレス]	on/off	off	ポートロックの例外を、有効または無効にします。
ip_filter_1 ～ ip_filter_8 [IP アドレス]	有効な IP アドレス	[空白]	ポートブロックから除外するネットワーク構成要素を IP アドレスで指定します。 **重要：** ワイルドカード (*) を使用すると、サブネットワークを指定できます。
hw_filter_on_1 ～ hw_filter_on_8 [MAC アドレス]	on/off	off	ポートロックの例外を、有効または無効にします。
hw_filter_1 ～ hw_filter_8 [MAC アドレス]	有効なハードウェアアドレス	00:00:00:00:00:00	ポートロックの対象から除外する要素を、MAC アドレス (ハードウェアアドレス) を使用して指定します。 **重要：** MAC アドレスはルータを通して配信されません。
protection_test [テストモード]	on/off	on	テストモードを有効または無効します。 **警告** テストモードでは、設定をテストするときにユーザ自身は除外されないように、初期値でアクティブに設定されています。UTN が再起動するまで設定はアクティブになり、以降のアクセスは制限されません。 設定のテストが正常に終了後、アクセス制御が正式に設定されるように、テストモードを非アクティブにする必要があります。

表35：パラメータリスト - USB 接続の暗号化

パラメータ	値	初期値	説明
utn_sec_1 ～ utn_sec_20 [USB ポート]	on/off	off	USB ポート (USB デバイスなど) とクライアント間の接続の SSL/TLS 暗号化を、有効または無効にします。 **重要：** ペイロードのみが暗号化されます。管理データおよびログデータは、暗号化せずに送信されます。

表36：パラメータリスト - USB デバイス種類のブロッキング

パラメータ	値	初期値	説明
utn_hid [入力デバイス (HID クラス) を無効にする]	on/off	on	入力デバイス (HID - ヒューマンインターフェイスデバイス) のブロッキングをアクティブまたは非アクティブにします。 on = ブロッキング無効 off= ブロッキング有効

表37：パラメータリスト - IPv4-VLAN (myUTN-80 以降のみ)

パラメータ	値	初期値	説明
utn_accctrt_1 ～ utn_accctrt_20 [方法]	--- ids key keyids	---	USB ポートと、ポートに接続された USB デバイスへのアクセスおよび使用を制限する方法を指定します。 ---= 制限なし ids= デバイス割り当て key= ポートキー制御 keyids= デバイス割り当て、およびキー制御
utn_keyval_1 ～ utn_keyval_20 [キー]	最大 64 半角文字 [a ～ z、A ～ Z、0 ～ 9]	[空白]	ポートキー制御を使用するときの、USB および接続された USB デバイスのキーを設定します。
utn_vendprodIDs_1 ～ utn_vendprodIDs_20 [USB デバイス]			デバイス割り当てにより USB ポートに割り当てられた USB デバイスの VID (ベンダ ID) と PID (製品 ID) を指定します。 USB デバイスの VID および PID は不明な場合が多いため、myUTN Control Center を使用することを推奨します。m y UTN Control Center を使用すると VID および PID が自動的に検出され入力されます。

表38：パラメータリスト - 認証

パラメータ	値	初期値	説明
auth_typ [認証方式]	--- MD5 TLS TTLS PEAP FAST	---	UTN サーバが参加するネットワーク内で使用される認証方式を設定します。 ---= なし MD5 = EAP-MD5 TLS = EAP-TLS TTLS = EAP-TTLS PEAP = PEAP FAST = EAP-FAST
auth_name [ユーザ名]	最大 64 半角文字 [a ～ z、A ～ Z、 0 ～ 9]	[空白]	RADIUS サーバ上で、EAP 認証方式の MD5、TTLS、PEAP および FAST 用に UTN サーバを設定するために使用するユーザ名を設定します。
auth_pwd [パスワード]	最大 64 半角文字 [a ～ z、A ～ Z、 0 ～ 9]	[空白]	RADIUS サーバ上で、EAP 認証方式の MD5、TTLS、PEAP および FAST 用に UTN サーバを設定するために使用するパスワードを設定します。
auth_intern [内部認証]	--- PAP CHAP MSCHAP2 EMD5 ETLS	---	EAP 認証方式の TTLS、PEAP および FAST に使用する内部認証の種類を指定します。 --- = なし PAP = PAP CHAP = CHAP MSCHAP2 = MS-CHAPv2 EMD5 = EAP-MD5 ETLS = EAP-TLS
auth_extern [PEAP/EAP-FAST オプション]	--- PLABEL0 PLABEL PVER0 PVER1 FPROV1	---	EAP 認証方式の TTLS、PEAP および FAST に使用する外部認証の種類を指定します。 ---= なし PLABEL0 = PEAPLABEL0 PLABEL1 = PEAPLABEL1 PVER0 = PEAPVER0 PVER1 = PEAPVER1 FPROV1 = FASTPROV1
auth_ano_name [匿名の名前]	最大 64 半角文字 [a ～ z、A ～ Z、 0 ～ 9]	[空白]	EAP 認証方式の TTLS、PEAP および FAST の非暗号化部分に使用する匿名の名前を指定します。
auth_wpa_addon [WPA アドオン]	最大 255 半角文字 [a ～ z、A ～ Z、 0 ～ 9]	[空白]	EAP 認証方式の TTLS、PEAP および FAST に使用する WPA 拡張を任意で指定します。

表39： パラメータリスト – バックアップ (myUTN-800 のみ)

パラメータ	値	初期値	説明
autoSync [パラメータのバックアップ]	on/off	on	パラメータ値、パスワードおよび証明書の、接続された SD カードへの自動バックアップを、有効または無効にします。

表40： パラメータリスト - その他

パラメータ	値	初期値	説明
utn_heartbeat	1 ～ 1800 [1 桁から 4 桁の数字：0 ～ 9]	180	**警告** このパラメータを使用するには、必ず SEH のサポートチームに相談してください。
utn_poffdur a_1 ～ utn_poffdur a_20	0 ～ 100 [1 ～ 3 個の半角文字：0 ～ 9]	0	**警告** このパラメータを使用するには、必ず SEH のサポートチームに相談してください。
utn_prereset_1 ～ utn_prereset_20	on/off	off	**警告** このパラメータを使用するには、必ず SEH のサポートチームに相談してください。

8.4 SEH UTN Manager – 機能の概要

SEH UTN Manager で非アクティブになる (グレイアウトされる) 機能は、次の様々な要因で決定されます。

- 選択リストモード
  - グローバル
  - ユーザ
- クライアントのオペレーティングシステム (Windows、macOS、Linux)
- クライアントユーザアカウント
  - 管理者または「utnusers」のグループメンバー
  - 標準ユーザまたは「utnusers」グループのメンバーでないユーザ
- *.ini ファイル (選択リスト) への書き込み権限

管理者は、ユーザに個別の機能を提供する際に、こうした要因を使用できます。

次の表に概略を示します。表に基本的に利用できる機能を示しています。また次の理由で、個別の機能が表示されない、または非アクティブとして表示されます。

- UTN サーバがその機能に対応していない
- 接続された USB デバイスがその機能に対応していない
- セキュリティ対策が実装されている

表41：SEH UTN Manager - 機能の概要、Linux

	グローバル選択リスト		ユーザ選択リスト		
	管理者	ユーザ	管理者	ユーザ (読み取り / 書き込み *.ini)	ユーザ (読み取り / 書き込みなし *.ini)
メニュー					
選択リスト - 編集	✓	×	✓	✓	×
選択リスト - エクスポート	✓	×	✓	×	×
選択リスト - リフレッシュ	✓	✓	✓	✓	✓
UTN サーバ - 構成	✓	✓	✓	✓	✓
UTN サーバ - IP アドレスの設定	✓	✓	✓	✓	✓
UTN サーバ - 自動接続の有効化	✓	×	✓	×	×
UTN サーバ - USB ポートキーの設定	✓	×	✓	✓	×
UTN サーバ - 追加	✓	×	✓	✓	×
UTN サーバ - 削除	✓	×	✓	✓	×
UTN サーバ - リフレッシュ	✓	✓	✓	✓	✓
ポート - 有効化	✓	✓	✓	✓	✓
ポート - 無効化	✓	✓	✓	✓	✓
ポート - リクエスト	✓	✓	✓	✓	✓
ポート - 削除	✓	×	✓	×	×
ポート - 設定	✓	✓	✓	✓	✓

	グローバル選択リスト		ユーザ選択リスト		
	管理者	ユーザ	管理者	ユーザ (読み取り / 書き込み *.ini)	ユーザ (読み取り / 書き込みなし *.ini)
ボタン					
選択リスト - リフレッシュ	✓	✓	✓	✓	✓
選択リスト - 編集	✓	×	✓	✓	×
ポート - 有効化	✓	✓	✓	✓	✓
ポート - 無効化	✓	✓	✓	✓	✓
「プログラム - オプション」ダイアログ					
ネットワークスキャン - マルチキャスト検索	✓	×	✓	×	×
ネットワークスキャン - IP 範囲検索	✓	×	✓	×	×
プログラム - プログラムメッセージ	✓	×	✓	×	×
プログラム - プログラムの更新	✓	×	✓	×	×
自動操作 - 自動切断	✓	×	✓	×	×
選択リスト - 選択リストモード	✓	×	✓	×	×
選択リスト - 自動リフレッシュ	✓	×	✓	×	×
「ポートの設定」ダイアログ					
メッセージ	✓	✓	✓	✓	✓